usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION
29TH USENIX SECURITY SYMPOSIUM

A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email

Hyeonmin Lee, Aniketh Gireesh, Roland van Rijswijk-Deij,
Taekyoung "Ted" Kwon, Taejoong Chung

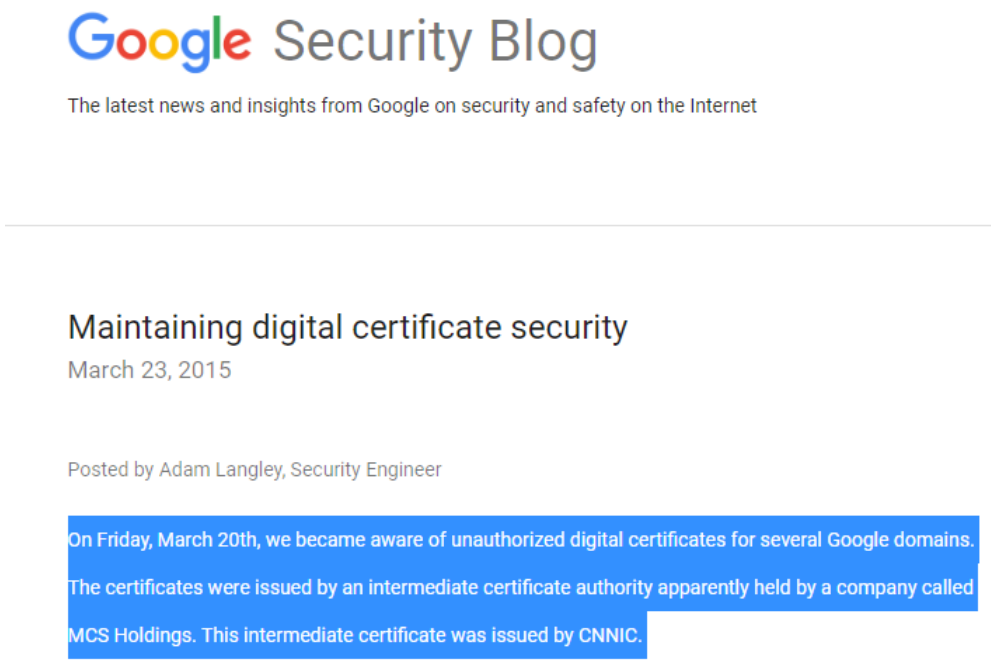
Seoul National University, Amrita Vishwa Vidyapeetham,
University of Twente & NLnet Labs, Virginia Polytechnic Institute and State University

The Problem of Public Key Infrastructure

- Some CAs were compromised and mis-issued fraudulent certificates for well-known domains

The Problem of Public Key Infrastructure

- Some CAs were compromised and mis-issued fraudulent certificates for well-known domains
  - e.g. CNNIC (2015), DigiNotar (2011), Comodo (2011), …



Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Maintaining digital certificate security

March 23, 2015

Posted by Adam Langley, Security Engineer

On Friday, March 20th, we became aware of unauthorized digital certificates for several Google domains. The certificates were issued by an intermediate certificate authority apparently held by a company called MCS Holdings. This intermediate certificate was issued by CNNIC.

DigiNotar SSL certificate hack amounts to cyberwar, says expert

Dutch government revokes certificates used for all its secure

BBC Sign in News Sport Reel Worklife Travel Future

NEWS

Home Video World Asia UK Business Tech Science Stories Entertainm

Technology

Fake DigiNotar web certificate risk to

The Problem of Public Key Infrastructure

- Some CAs were compromised and mis-issued fraudulent certificates for well-known domains
  - e.g. CNNIC (2015), DigiNotar (2011), Comodo (2011), …

Can we trust all these CAs?

The Problem of Public Key Infrastructure

Suggested countermeasures

- Certificate Transparency (CT)
- Certification Authority Authorization (CAA)
- …

The Problem of Public Key Infrastructure

Suggested countermeasures

- Certificate Transparency (CT)
- Certification Authority Authorization (CAA)
- …

Do not fundamentally solve the problem!

Still rely on CAs

What is DANE?

DNS-based Authentication of Named Entities (DANE)

- An Internet security protocol which allows certificates to be bound to domain names
  - Publish certificate information as a DNS record (**TLSA record**)

DNS-based Authentication of Named Entities (DANE)

- An Internet security protocol which allows certificates to be bound to domain names
  - Publish certificate information as a DNS record (TLSA record)

- The Domain Name System Security Extensions (DNSSEC) is used to guarantee the integrity and authenticity of TLSA records

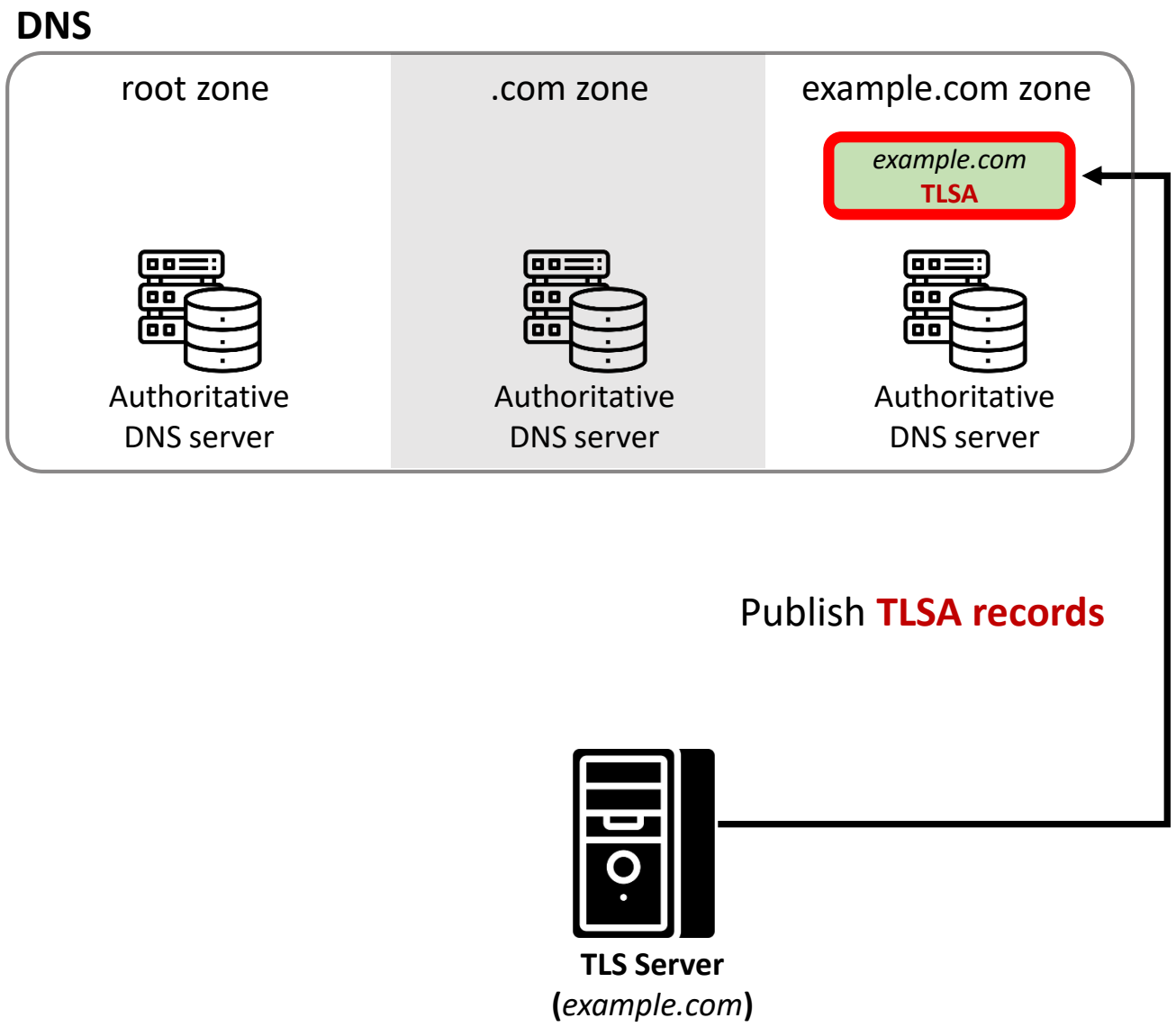
DNS-based Authentication of Named Entities (DANE)

- An Internet security protocol which allows certificates to be bound to domain names
  - Publish certificate information as a DNS record (TLSA record)

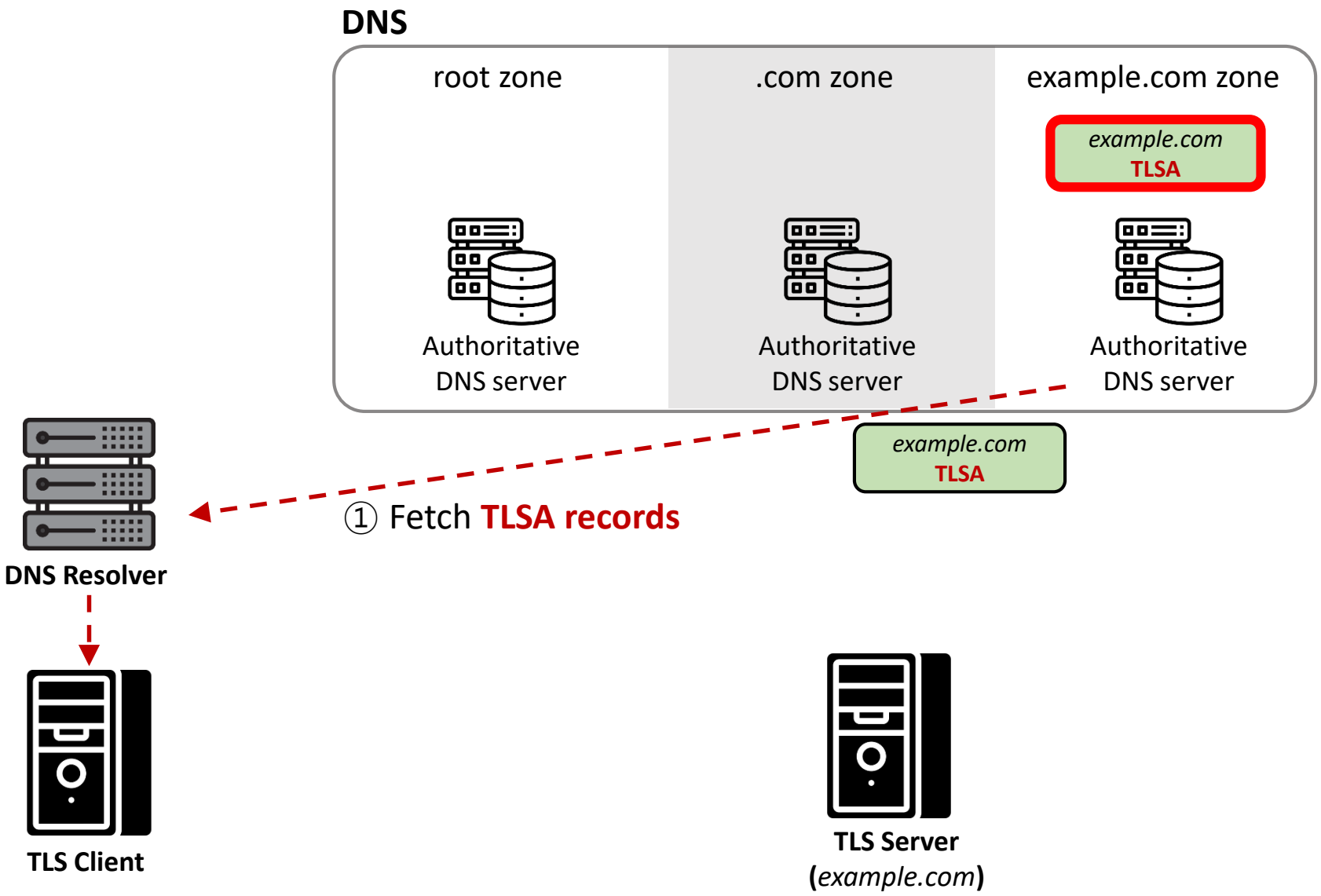
- The Domain Name System Security Extensions (DNSSEC) is used to guarantee the integrity and authenticity of TLSA records

Support TLS without relying on trusted third-parties like CAs

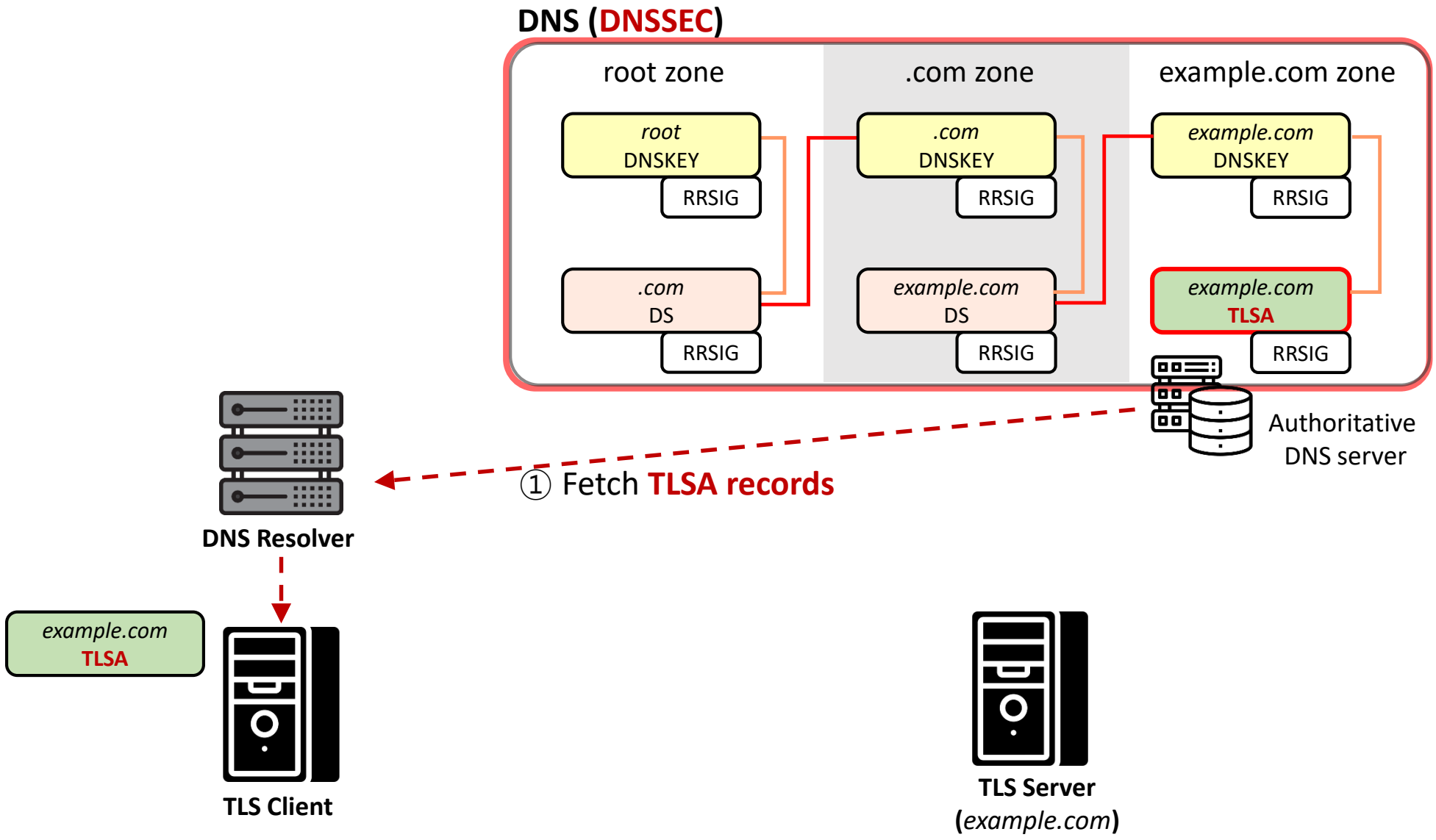
DNS-based Authentication of Named Entities (DANE)



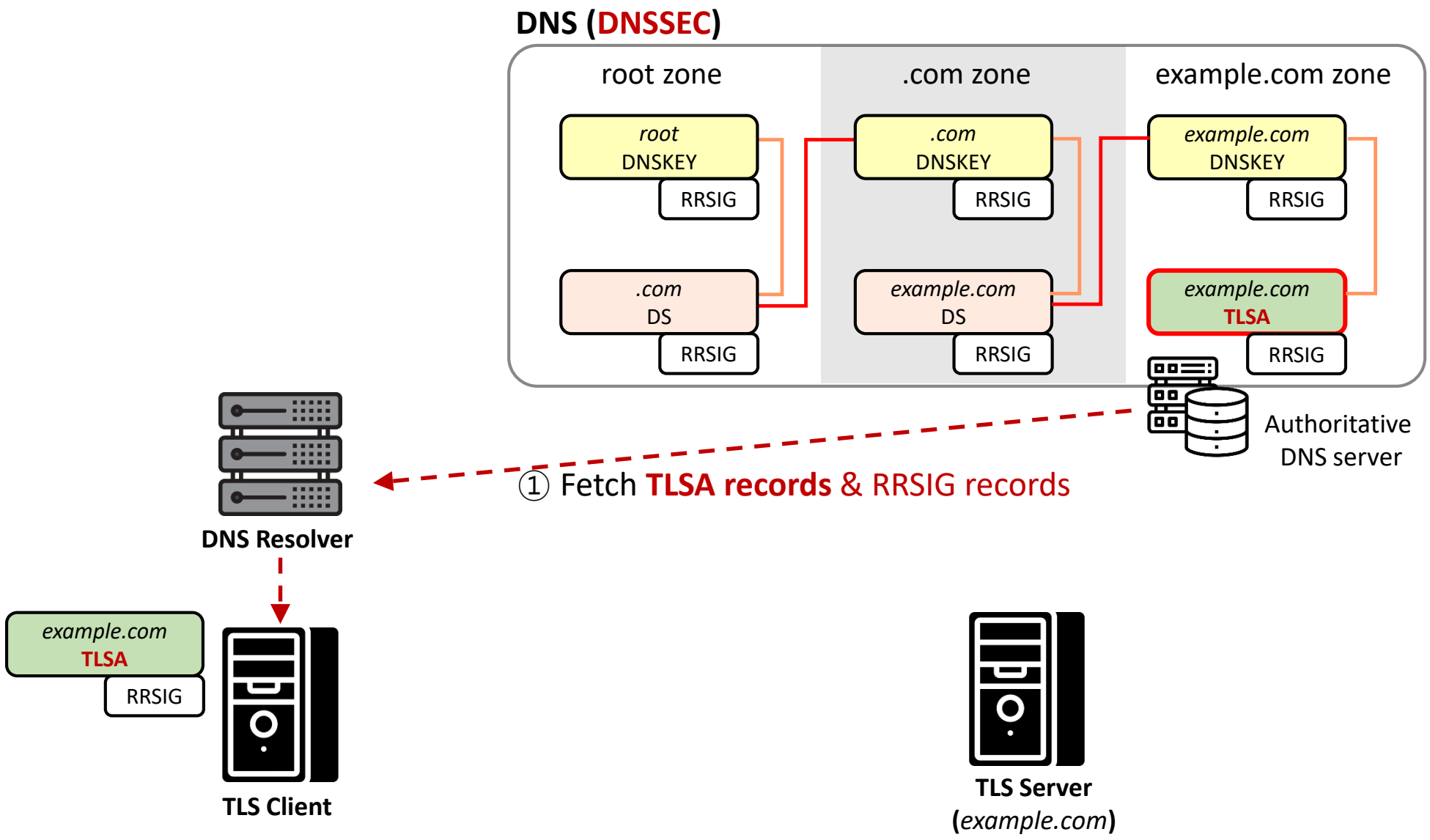
DNS-based Authentication of Named Entities (DANE)



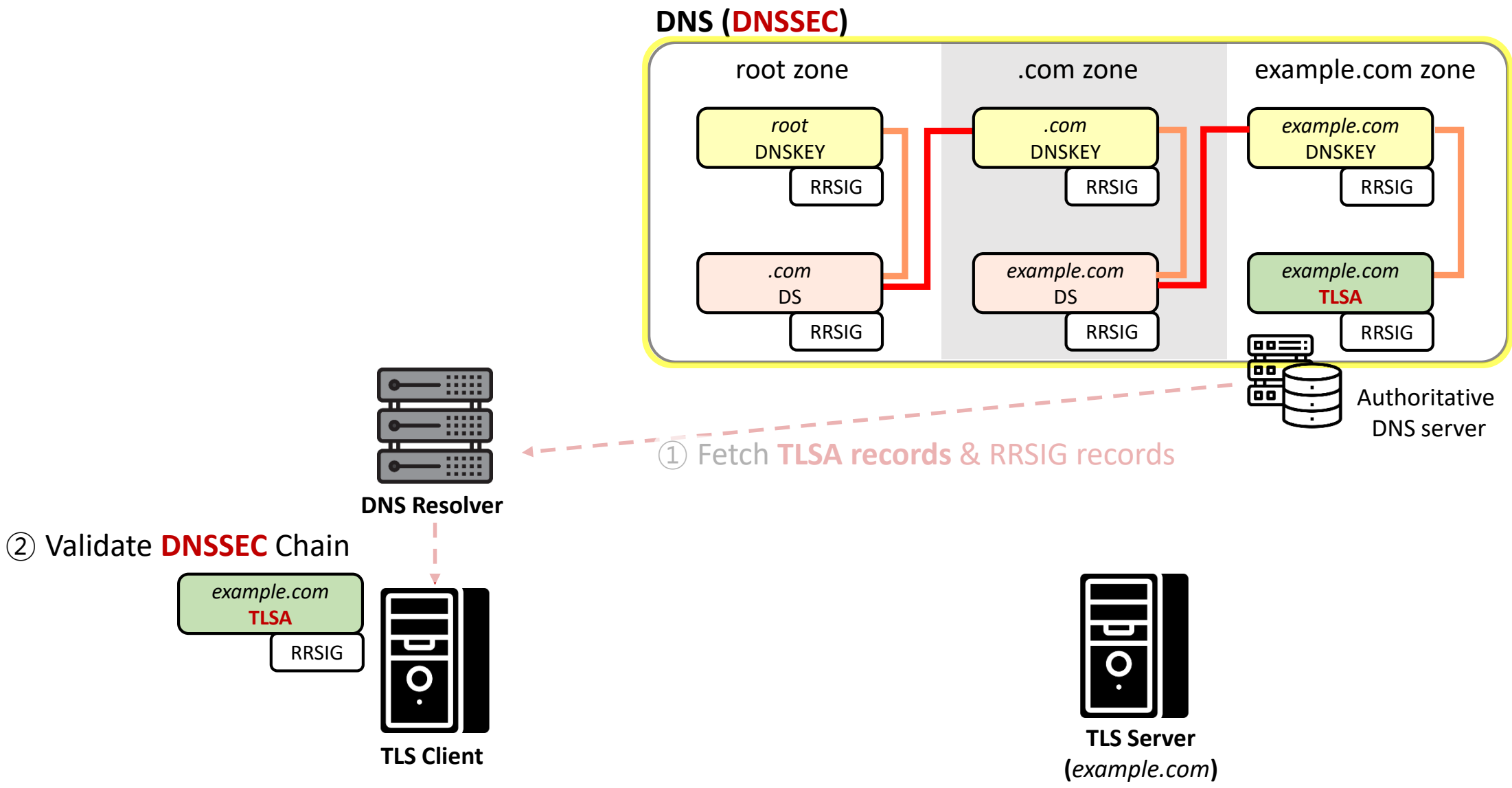
DNS-based Authentication of Named Entities (DANE)



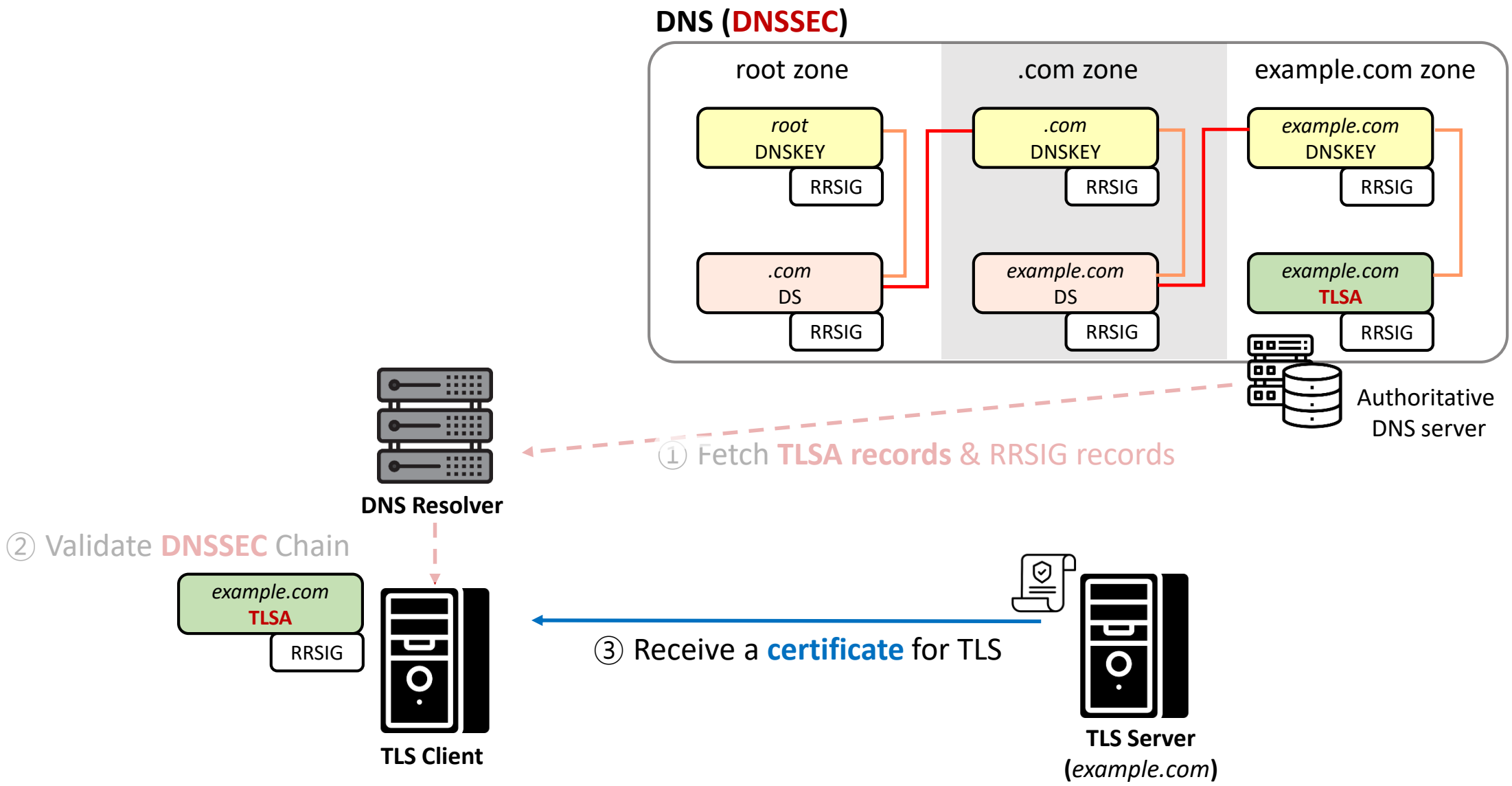
DNS-based Authentication of Named Entities (DANE)



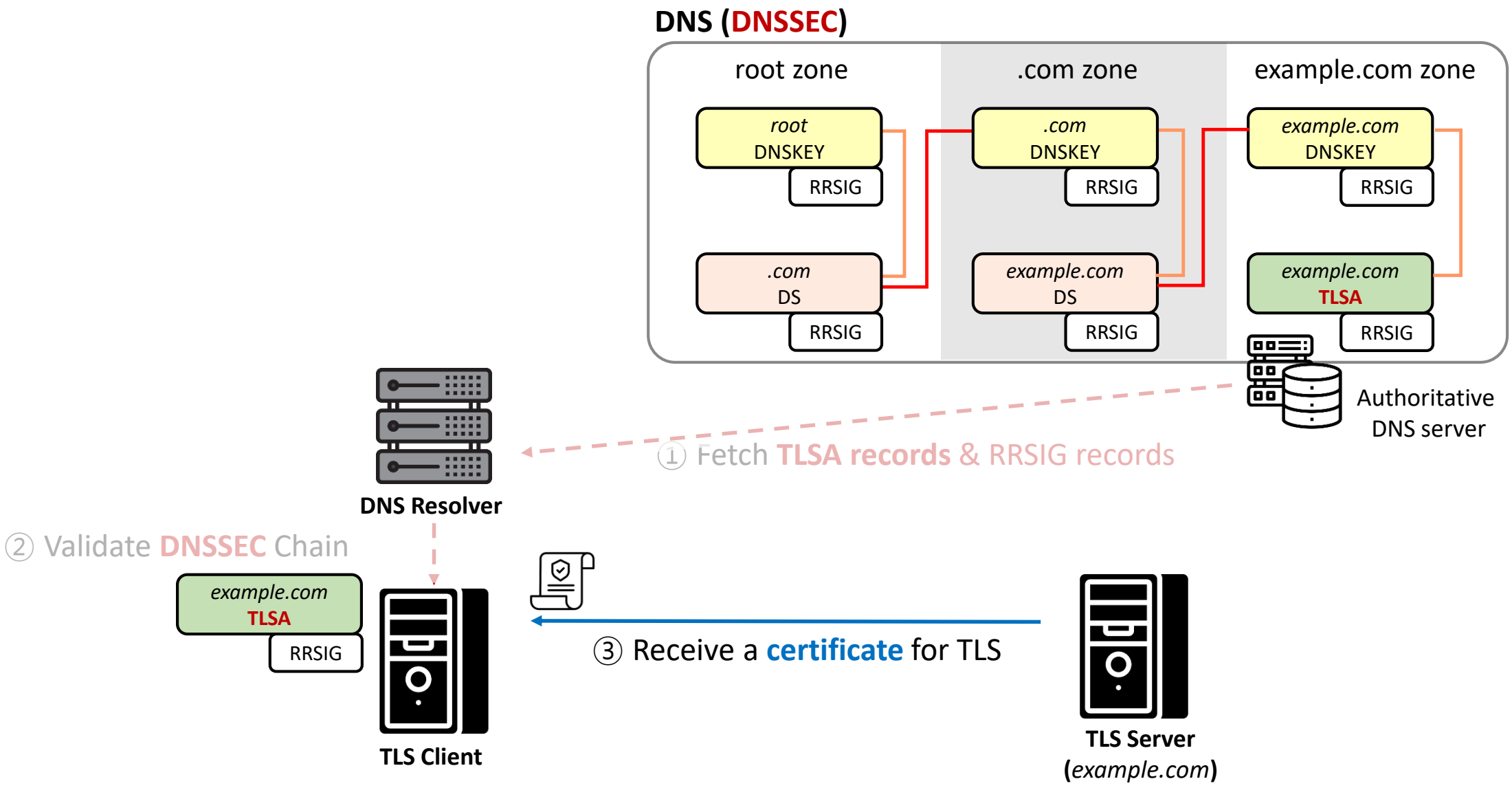
DNS-based Authentication of Named Entities (DANE)



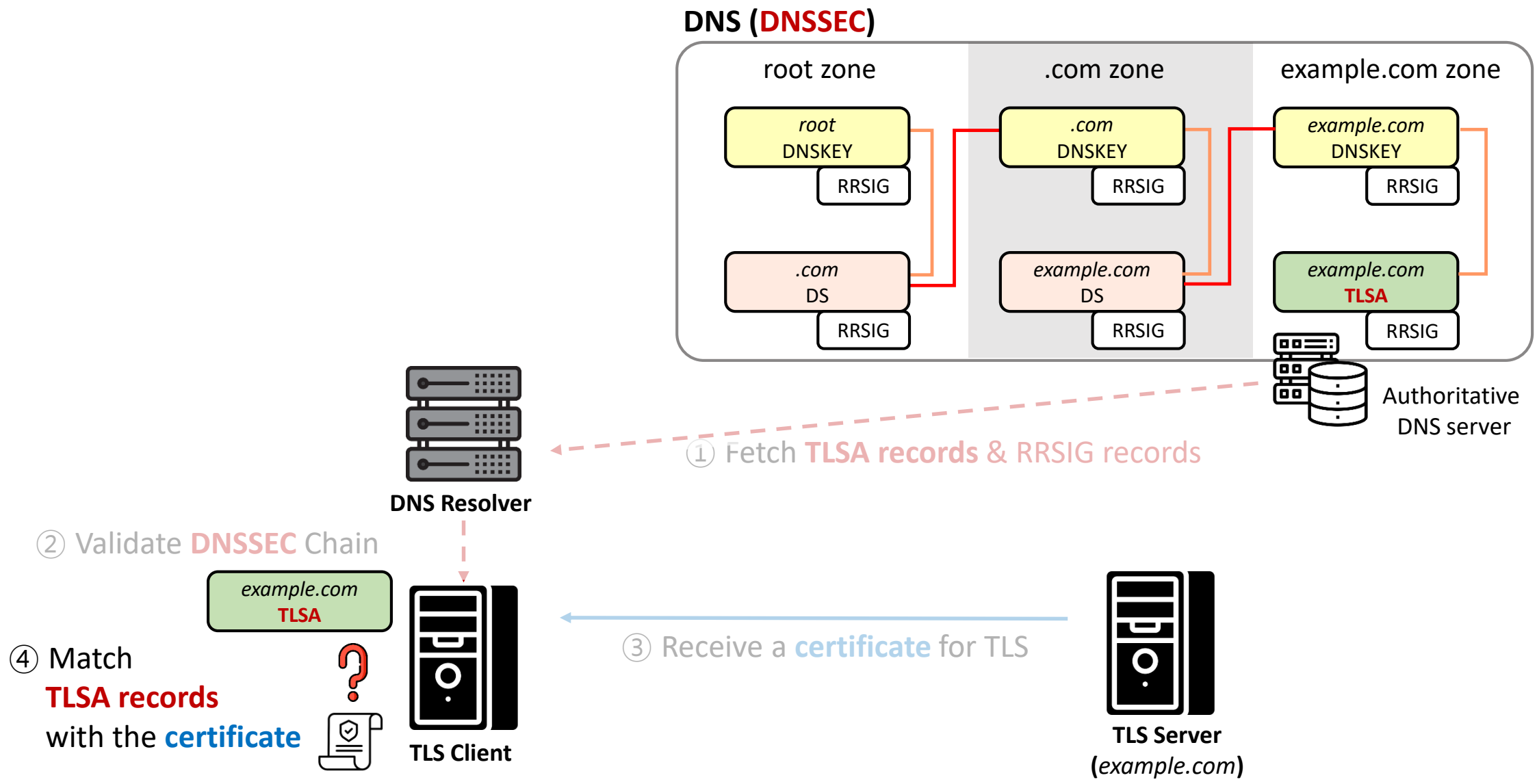
DNS-based Authentication of Named Entities (DANE)



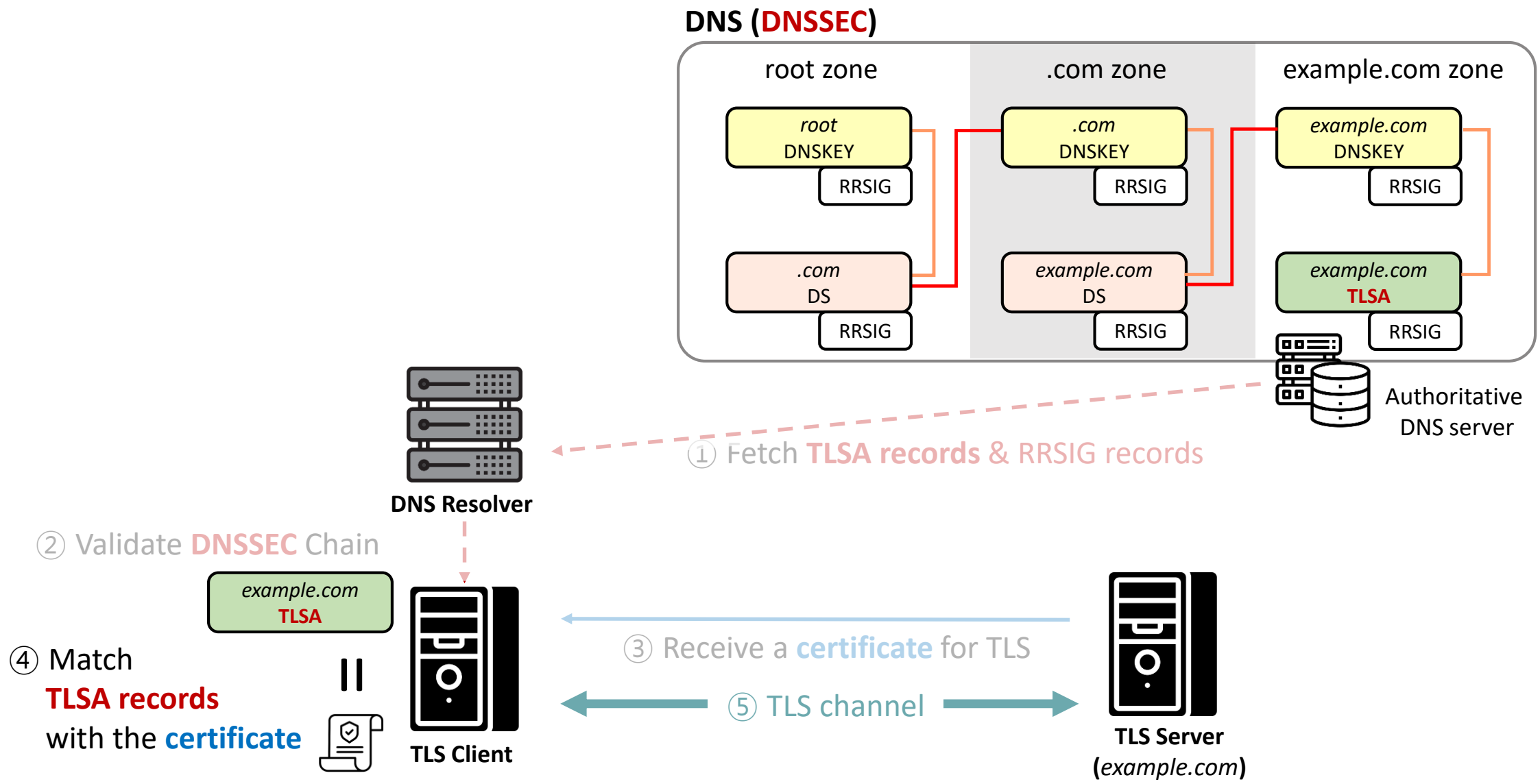
DNS-based Authentication of Named Entities (DANE)



DNS-based Authentication of Named Entities (DANE)



DNS-based Authentication of Named Entities (DANE)



Where DANE is used?

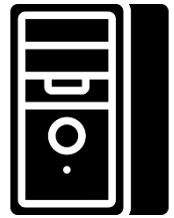
DANE + SMTP Background

- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism

DANE + SMTP Background

- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection

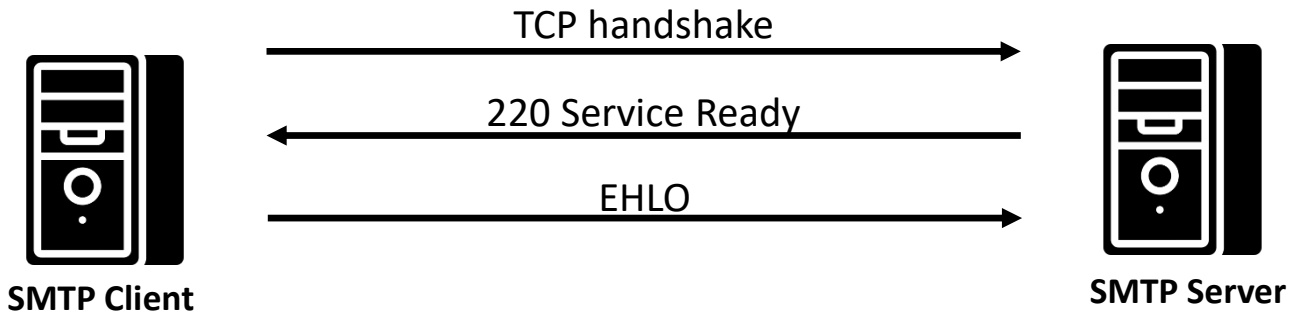
SMTP Client



SMTP Server

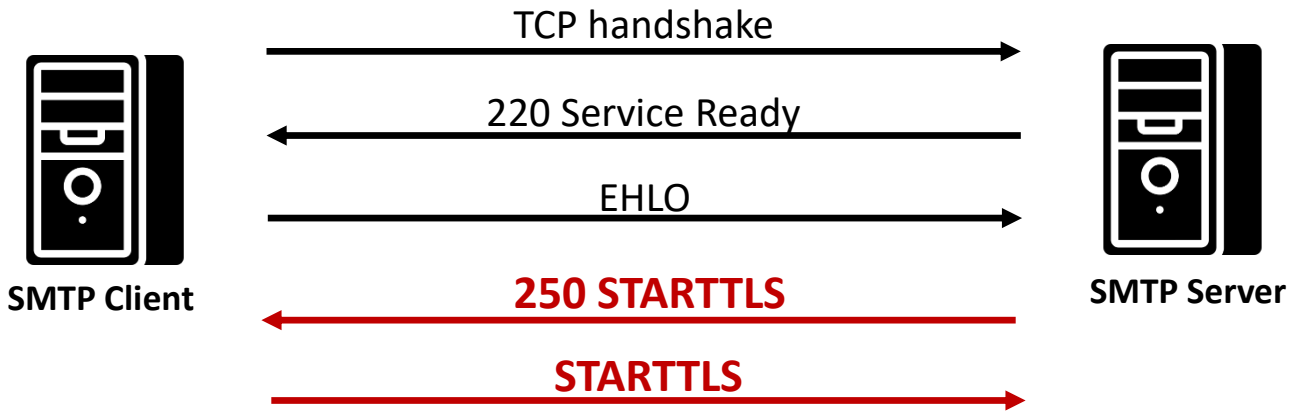
DANE + SMTP Background

- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection



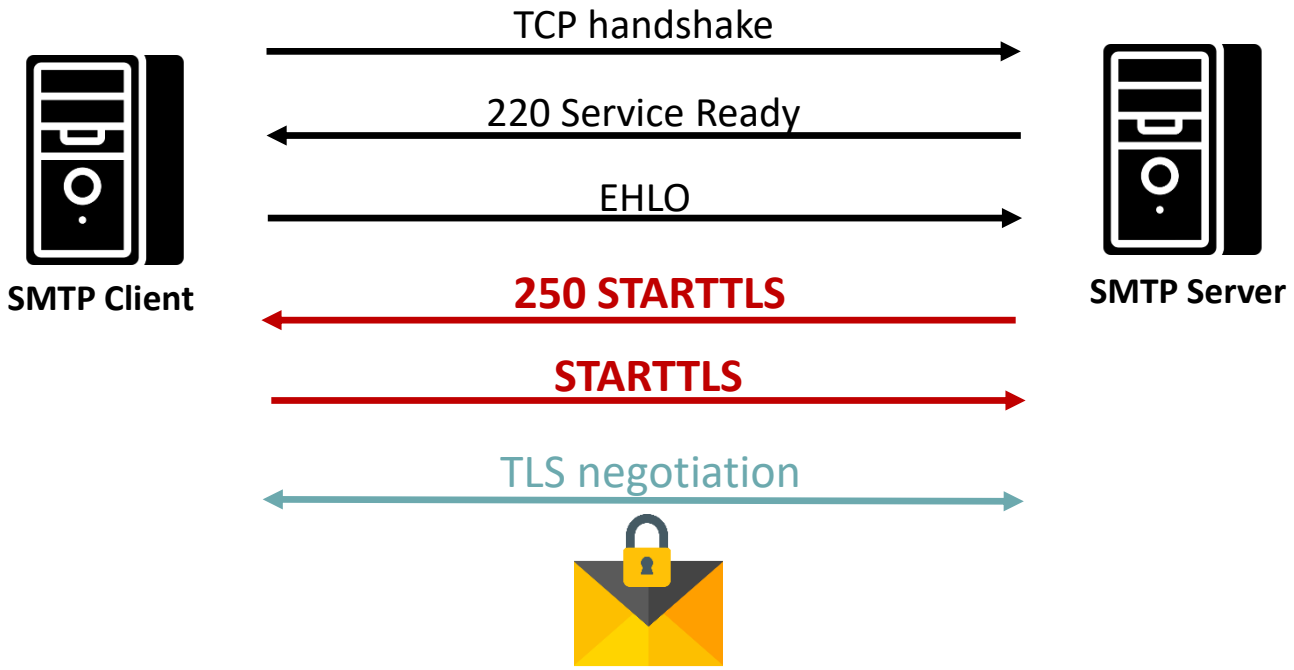
DANE + SMTP Background

- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection



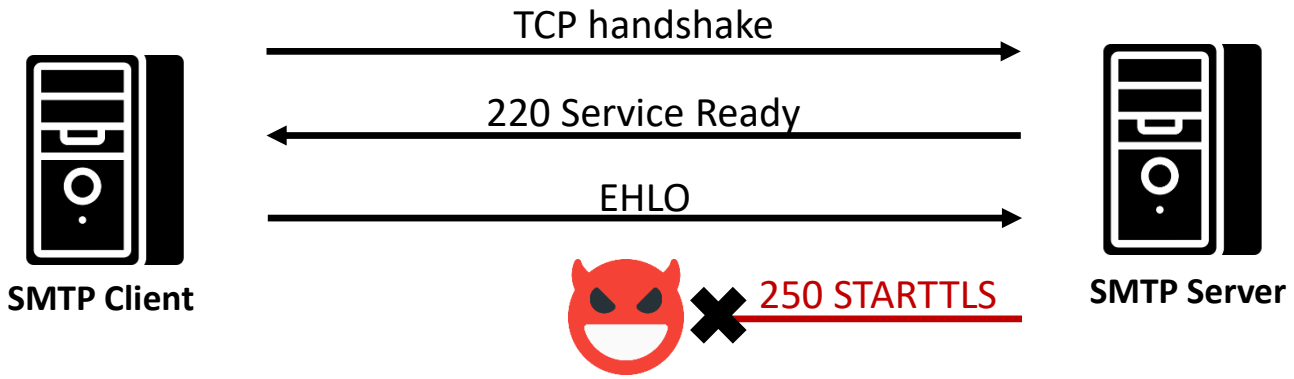
DANE + SMTP Background

- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection



DANE + SMTP Background

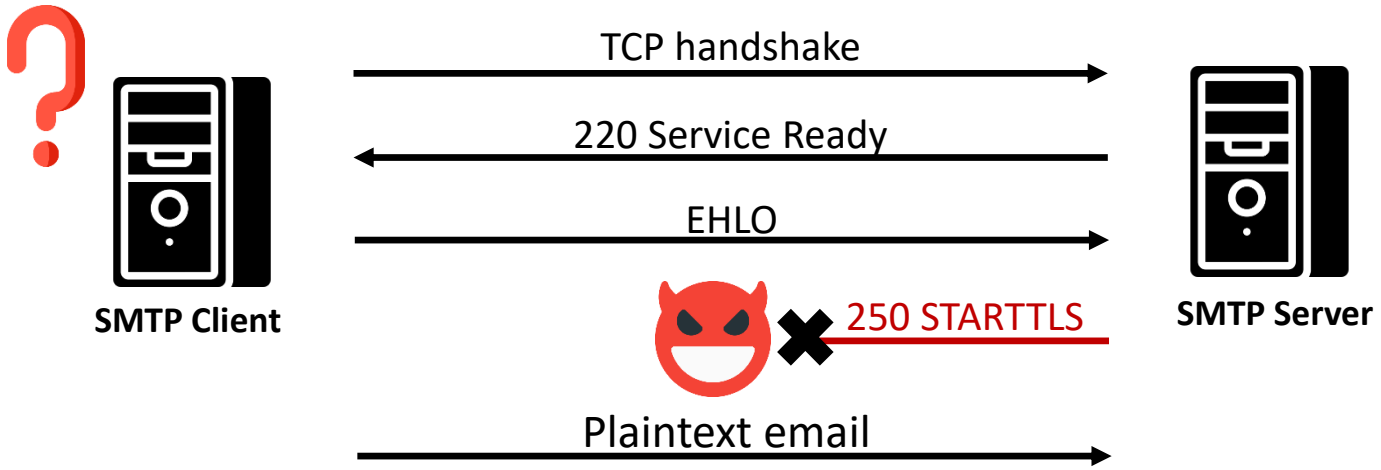
- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection



Vulnerable to downgrade attacks

DANE + SMTP Background

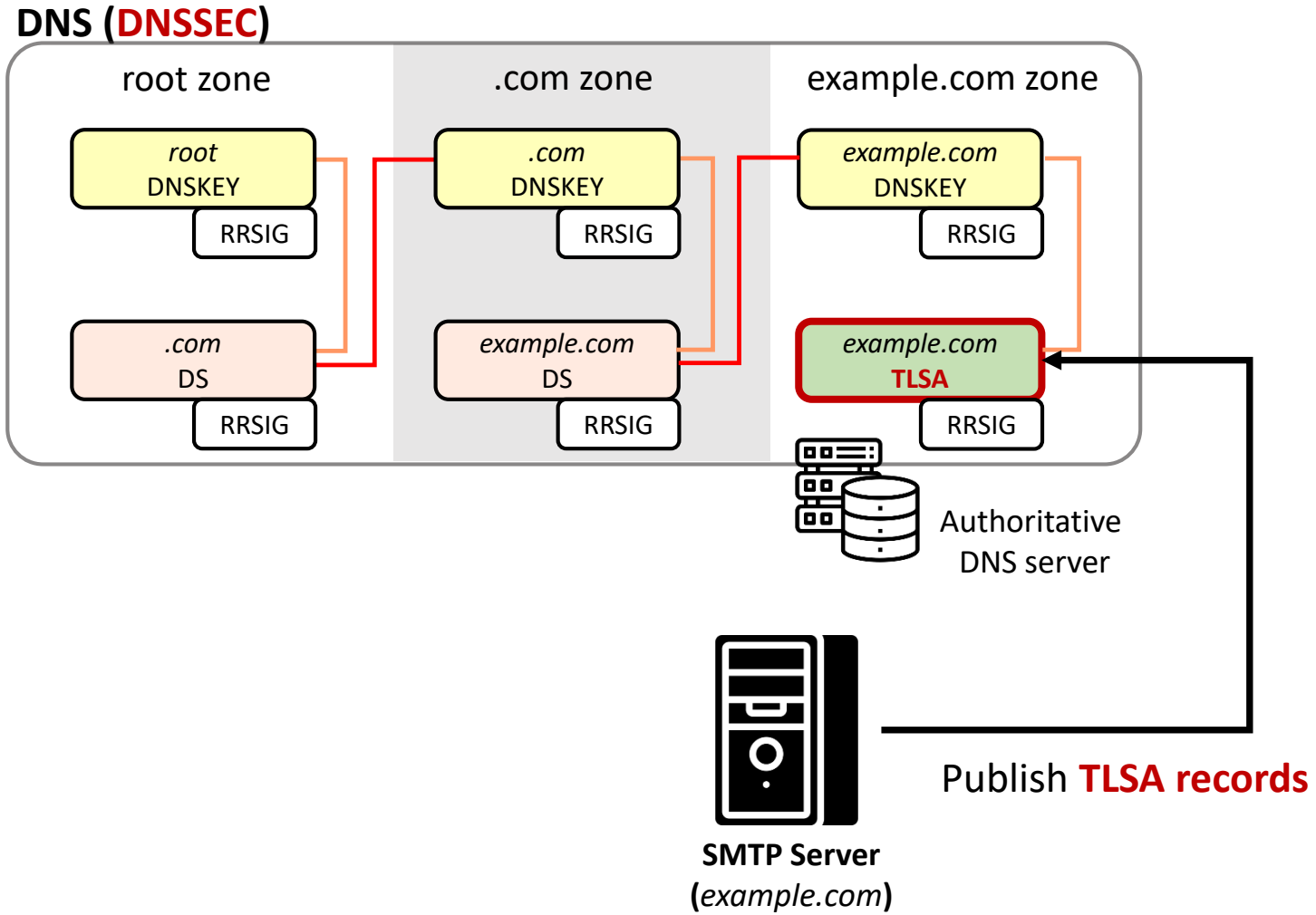
- Simple Mail Transfer Protocol (SMTP) has no built-in security mechanism
- STARTTLS supports opportunistic TLS for SMTP connection



Vulnerable to downgrade attacks

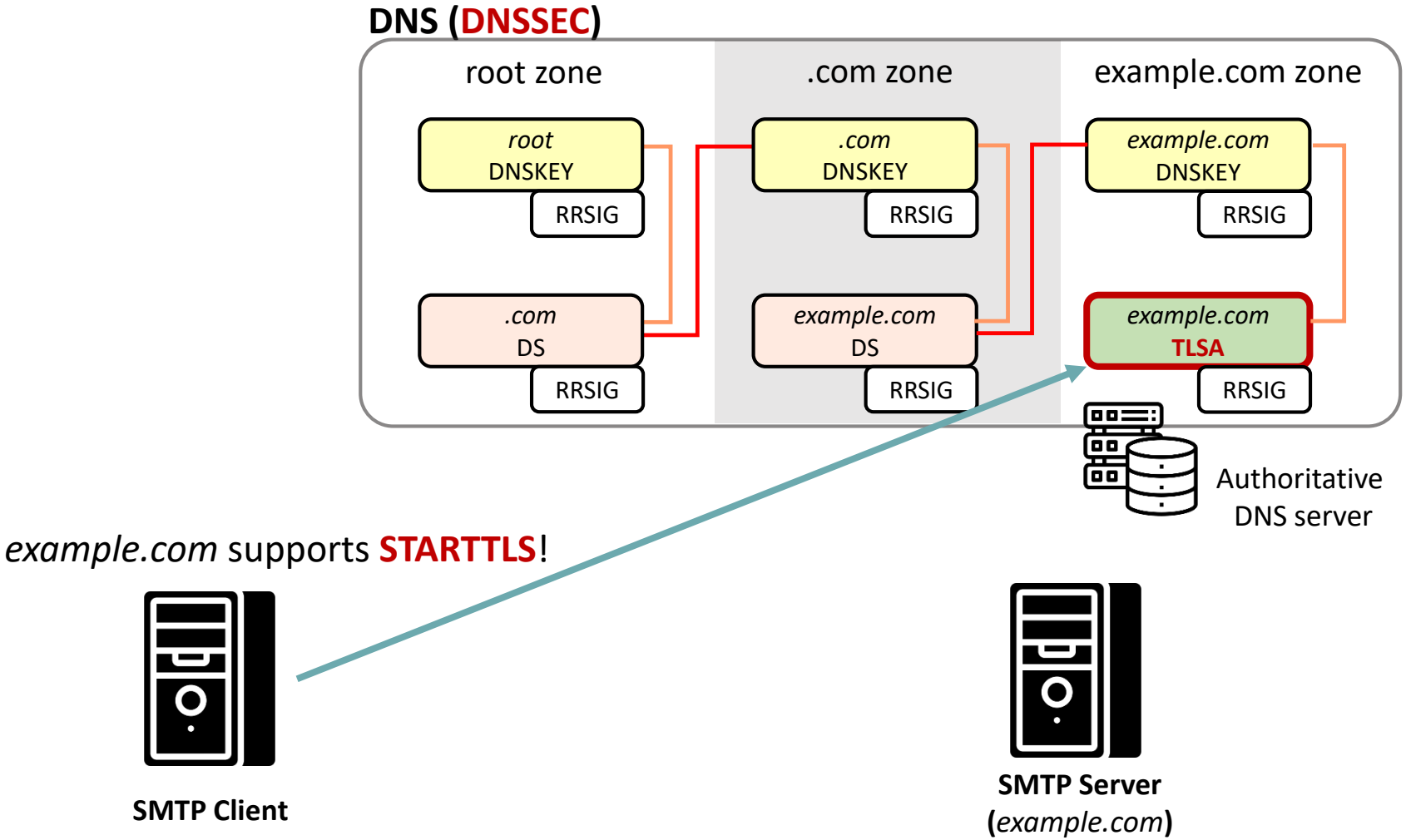
DANE + SMTP

- With DANE, STARTTLS downgrade attack can be mitigated



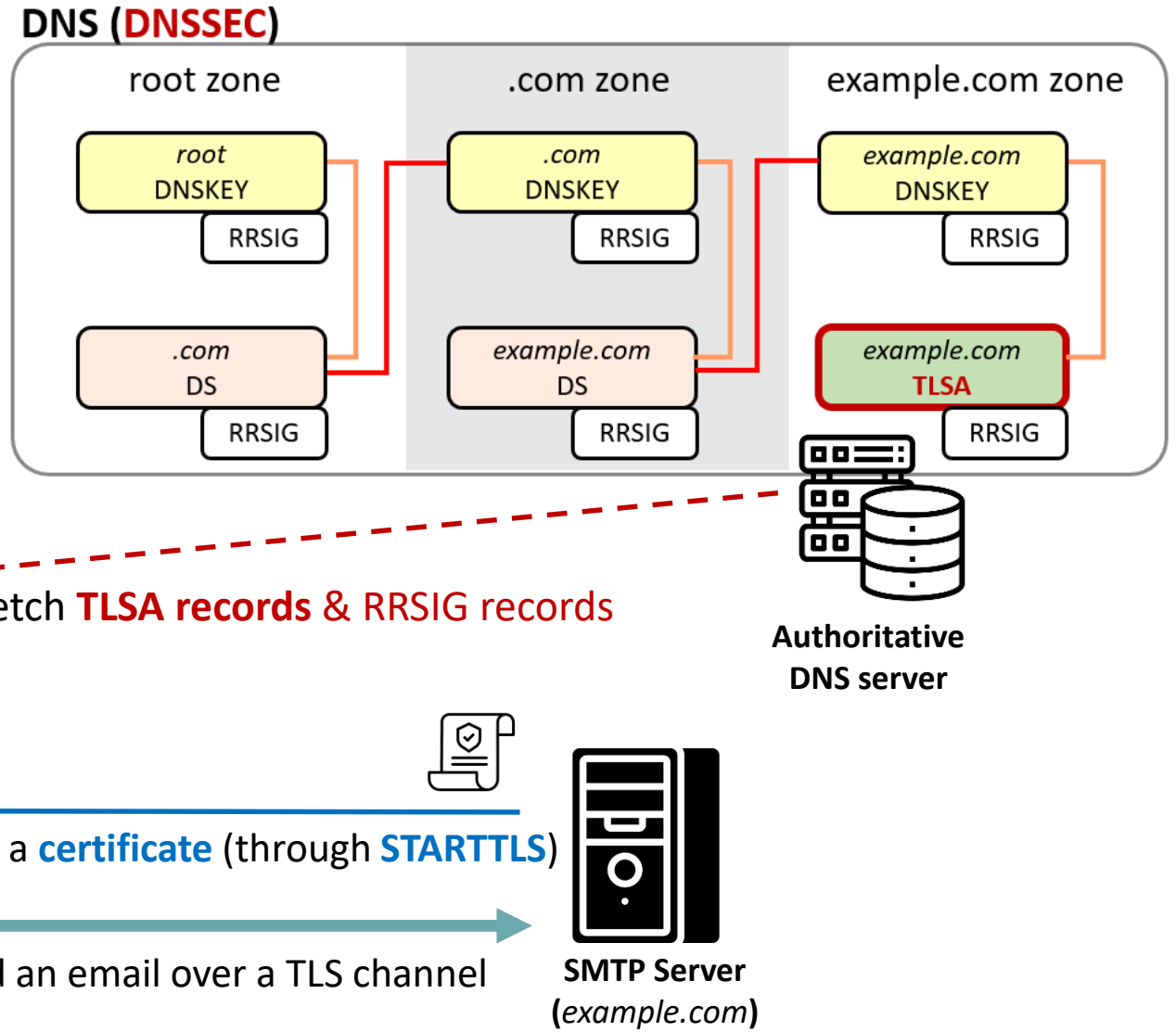
DANE + SMTP

- With DANE, STARTTLS downgrade attack can be mitigated



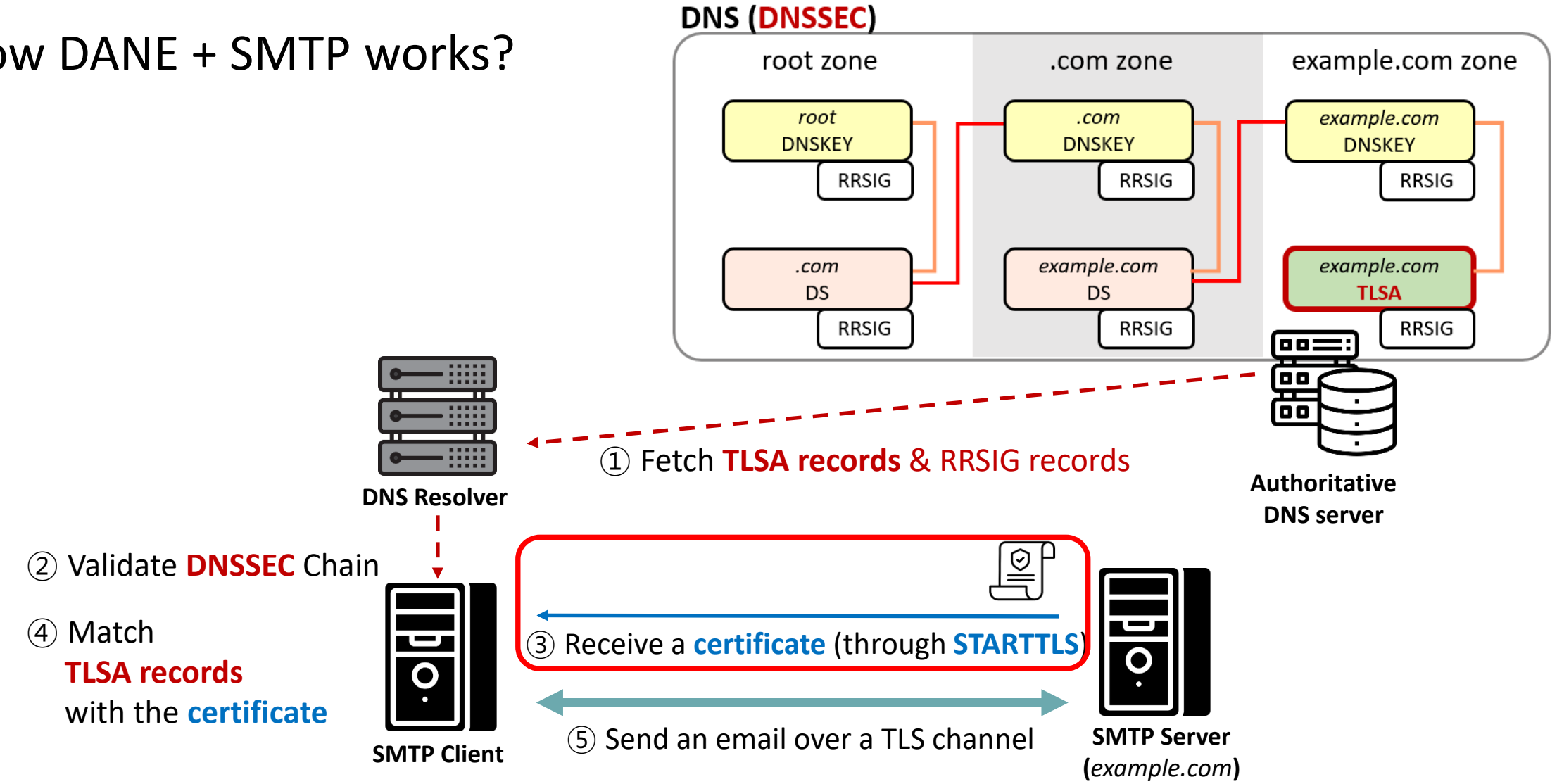
DANE + SMTP

- How DANE + SMTP works?

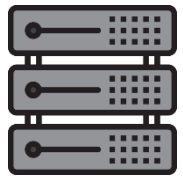


DANE + SMTP

- How DANE + SMTP works?



Understanding of DANE Ecosystem



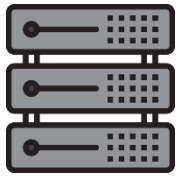
DNS Resolver

Authoritative
DNS server

SMTP Client

SMTP Server

Understanding of DANE Ecosystem



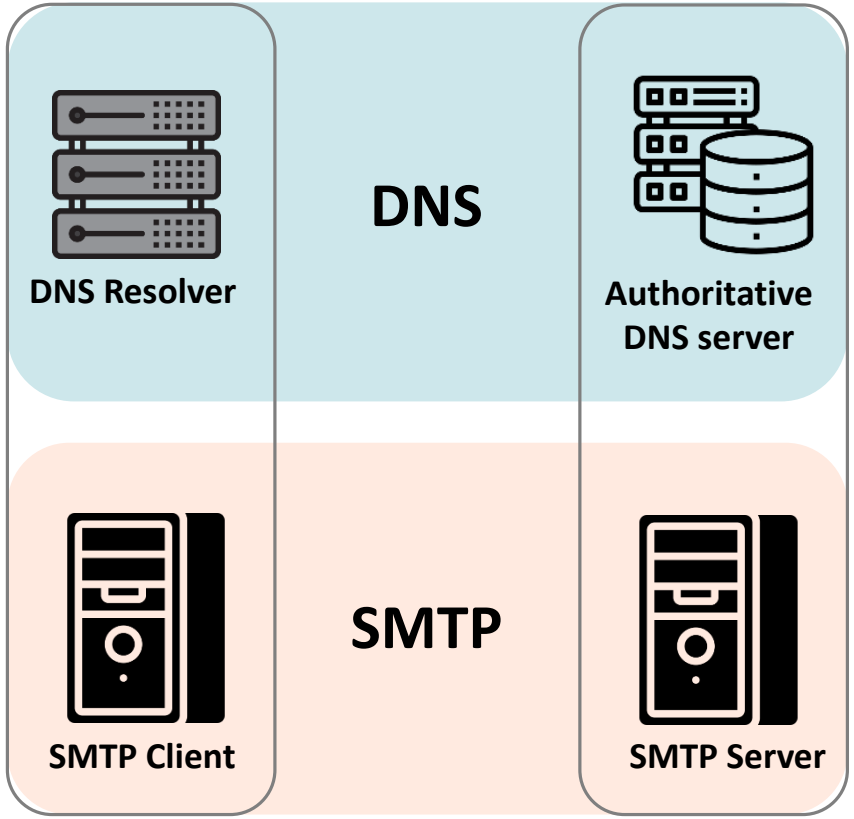
DNS Resolver

Authoritative
DNS server

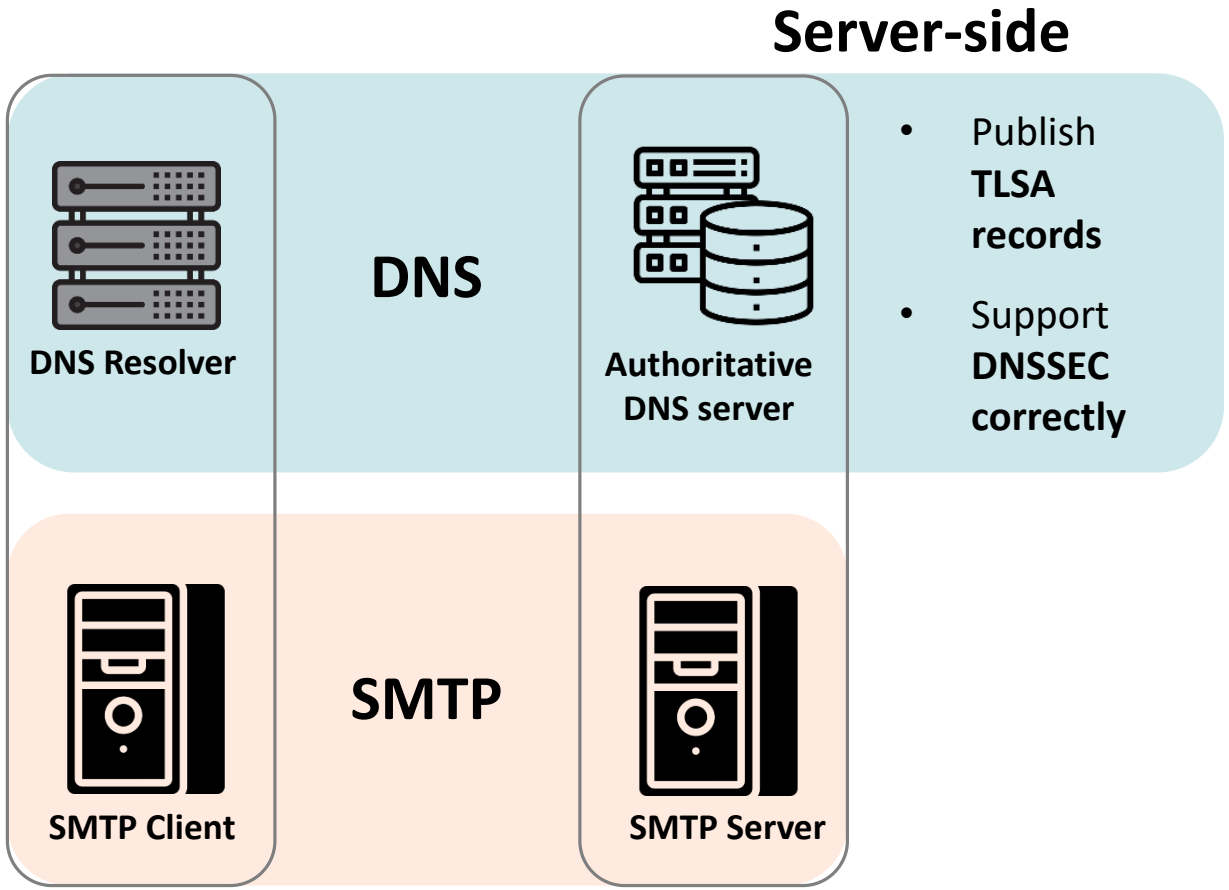
SMTP Client

SMTP Server

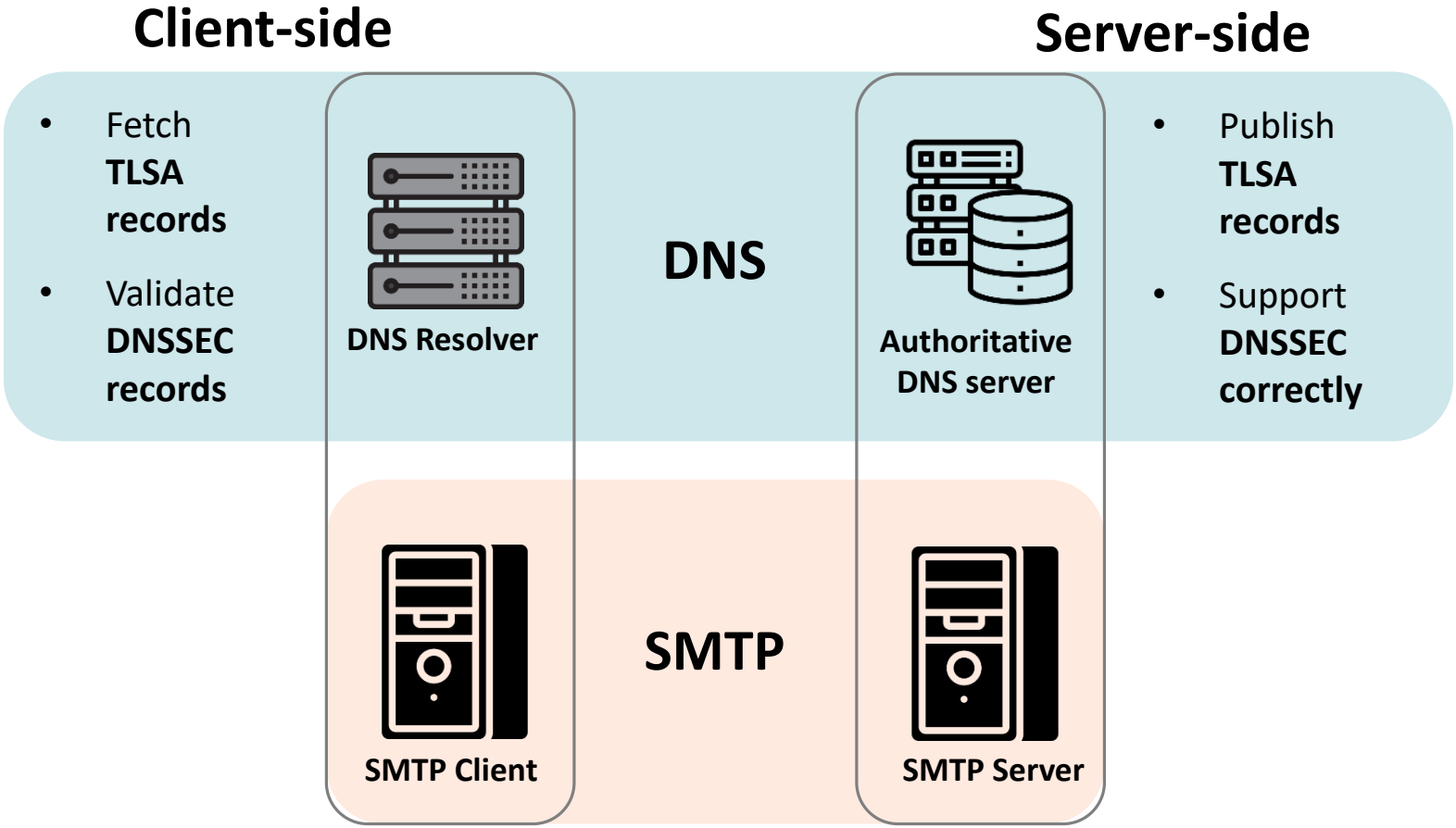
Understanding of DANE Ecosystem



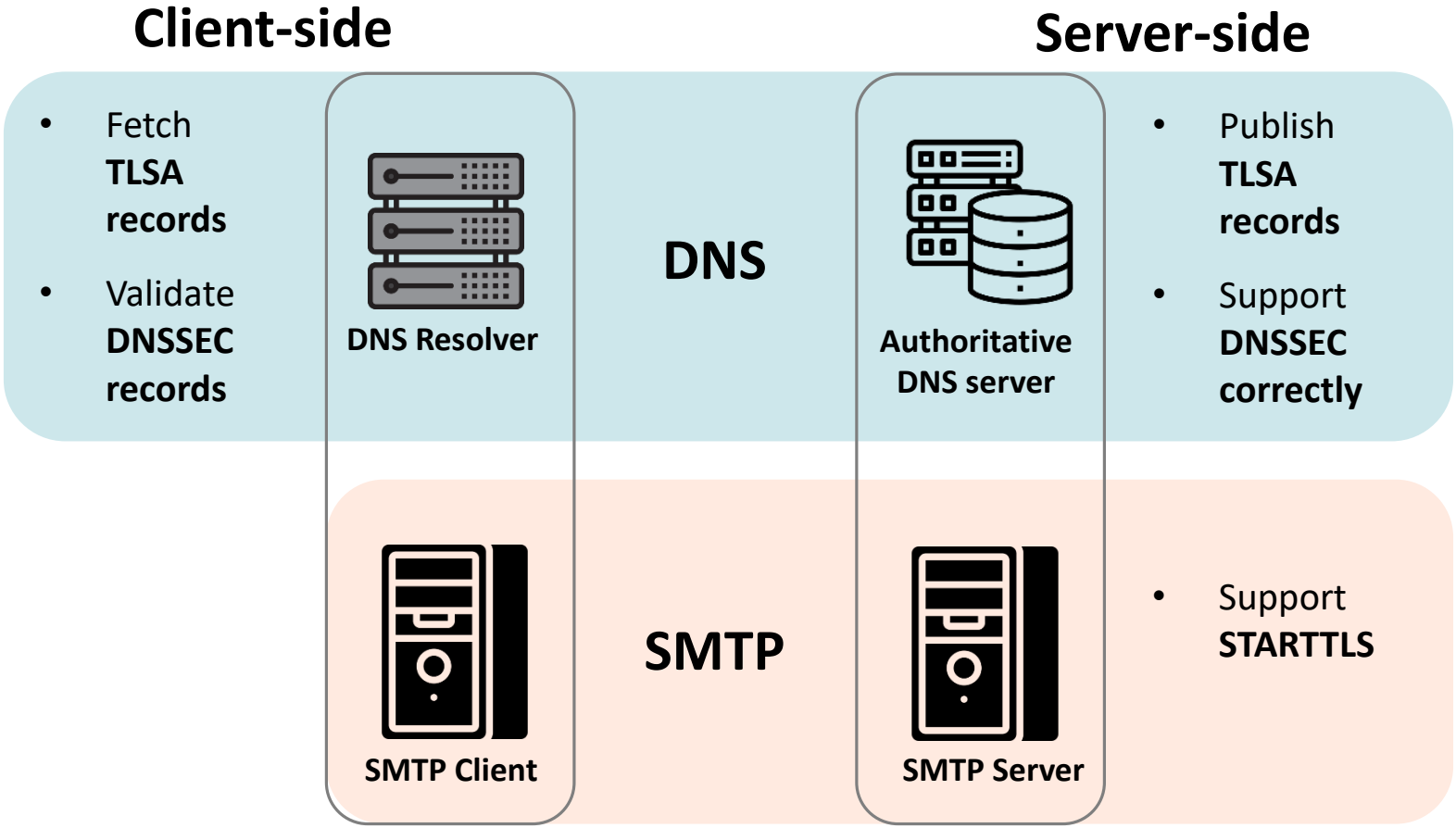
Understanding of DANE Ecosystem



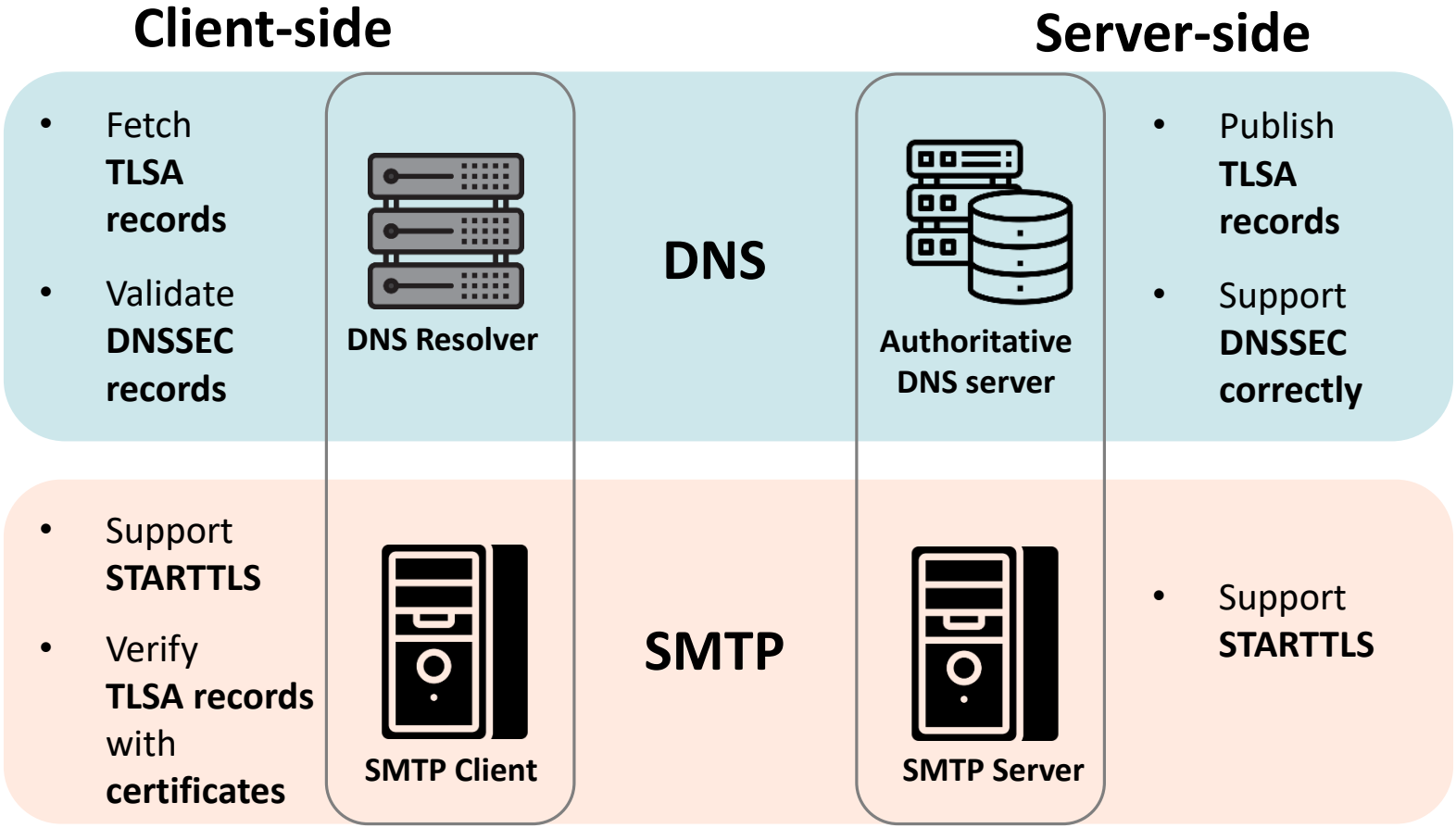
Understanding of DANE Ecosystem



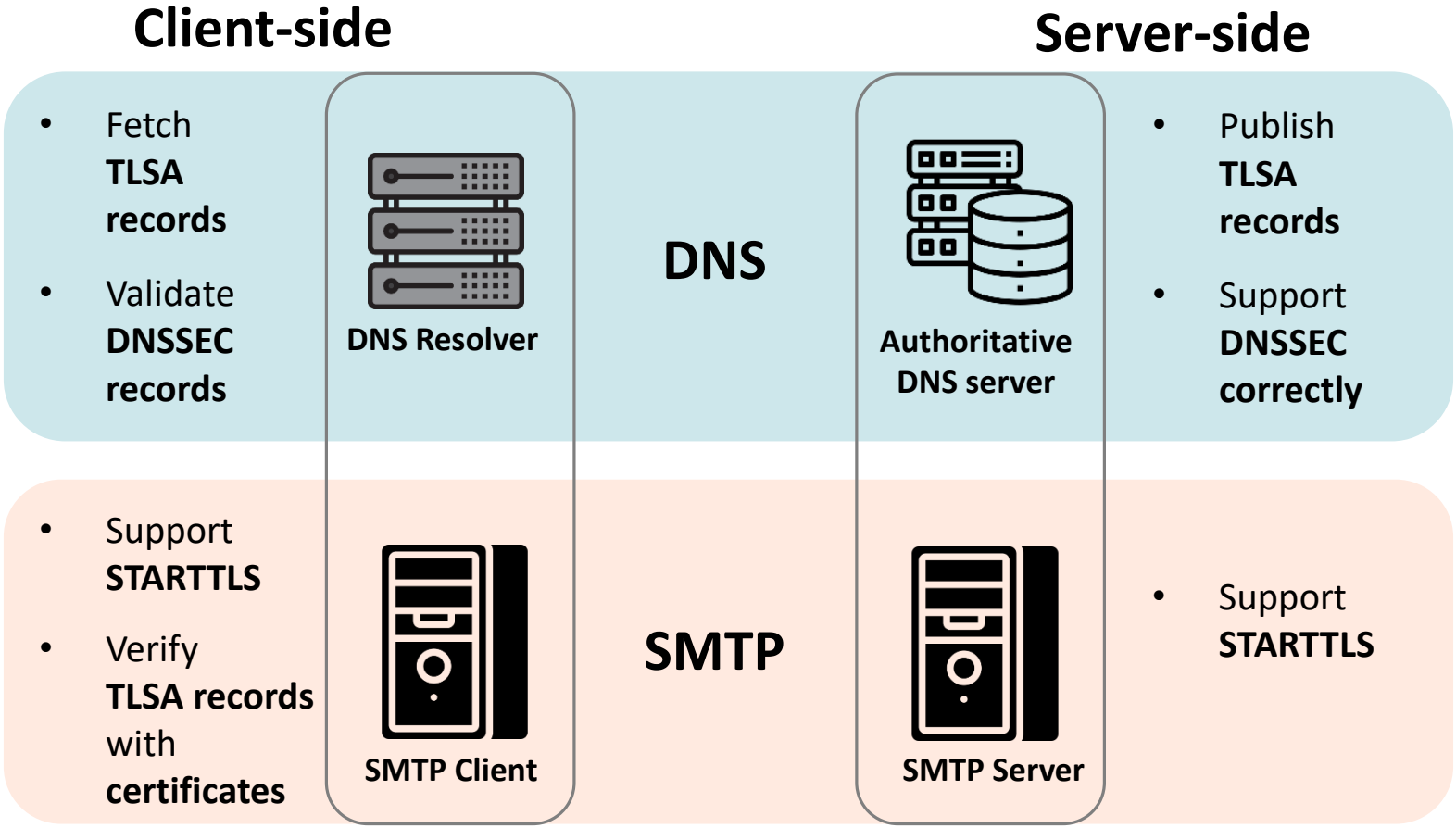
Understanding of DANE Ecosystem



Understanding of DANE Ecosystem

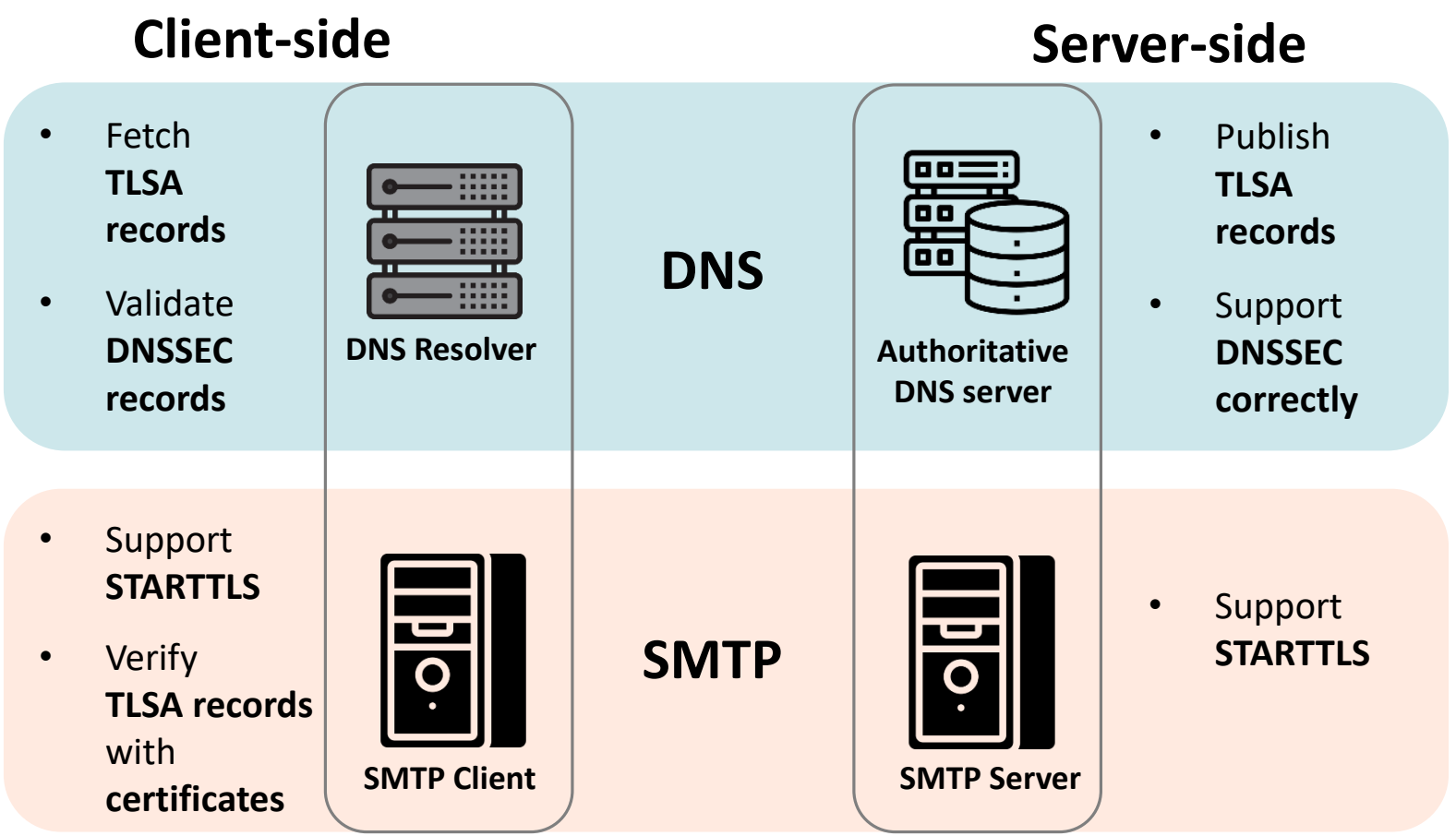


Understanding of DANE Ecosystem



DANE can only function correctly
when all entities fulfill their responsibilities

Understanding of DANE Ecosystem

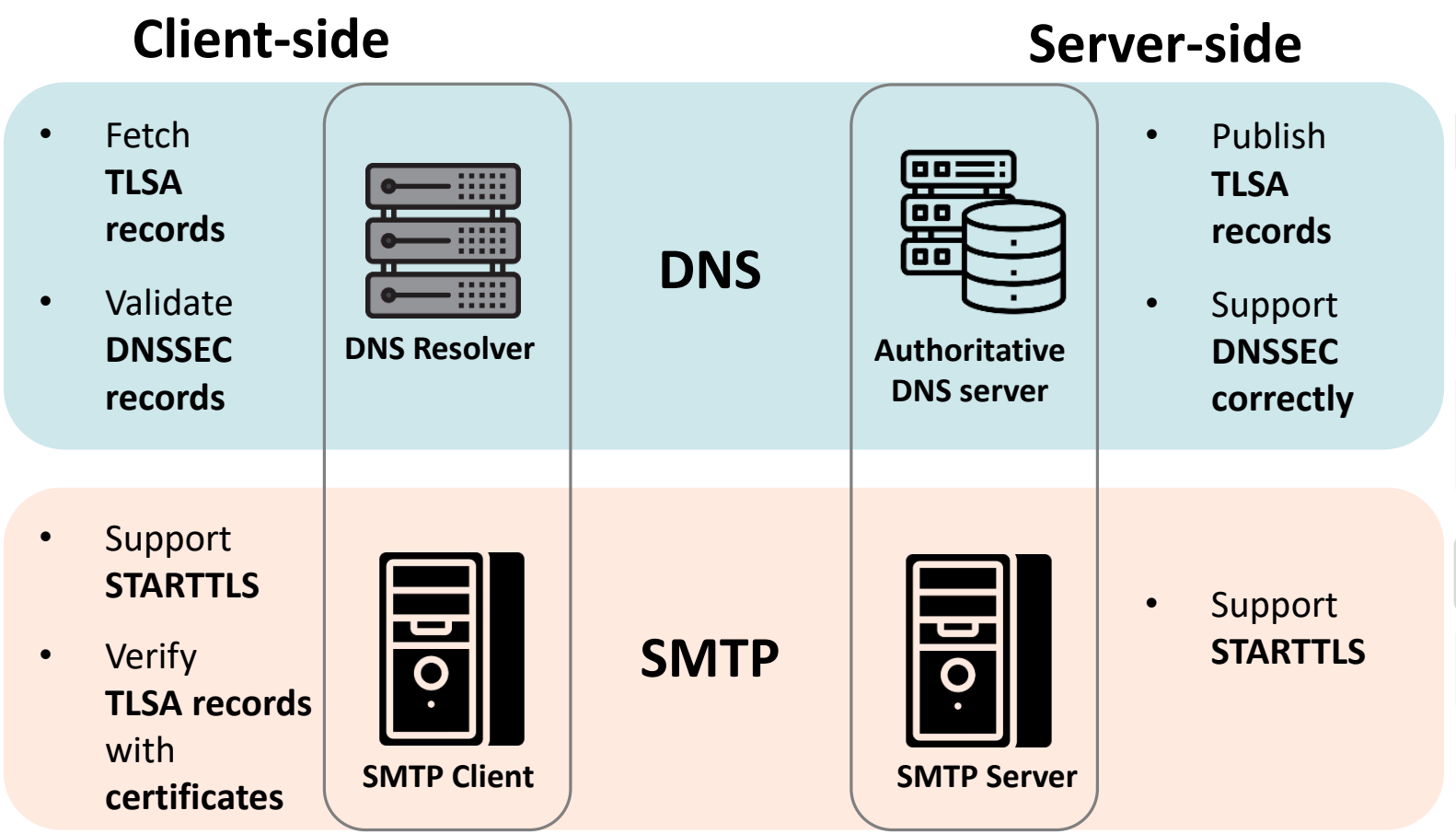


Analysis

Deployment
TLSA
2 years Every Day
5 TLD* *.com, .net, .org* *.se, .nl*

*OpenINTEL (https://openintel.nl/)

Understanding of DANE Ecosystem



Analysis

Deployment
TLSA
2 years Every Day
5 TLD* *.com, .net, .org* *.se, .nl*
Management
TLSA Certificate
4 months Every Hour

*OpenINTEL (https://openintel.nl/)

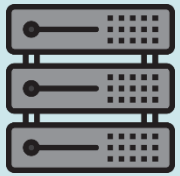
Understanding of DANE Ecosystem

Analysis

Popular Email Service Providers

Client-side

- Fetch **TLSA records**
- Validate **DNSSEC records**



DNS Resolver

DNS

Server-side

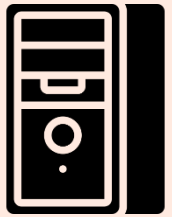
Authoritative DNS server

- Publish **TLSA records**
- Support **DNSSEC correctly**

- Support **STARTTLS**
- Verify **TLSA records** with **certificates**

SMTP Client

SMTP



SMTP Server

- Support **STARTTLS**

Analysis

Deployment
TLSA
2 years Every Day
5 TLD* *.com, .net, .org* *.se, .nl*
Management
TLSA Certificate
4 months Every Hour

*OpenINTEL (https://openintel.nl/)

Understanding of DANE Ecosystem

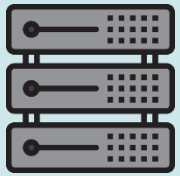
Analysis

Popular Email Service Providers

Popular MTA and DNS Software

Client-side

- Fetch **TLSA records**
- Validate **DNSSEC records**



DNS Resolver

DNS

Authoritative DNS server

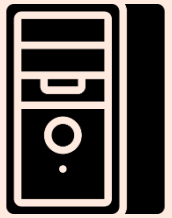
Server-side

- Publish **TLSA records**
- Support **DNSSEC correctly**

- Support **STARTTLS**
- Verify **TLSA records** with **certificates**

SMTP Client

SMTP



SMTP Server

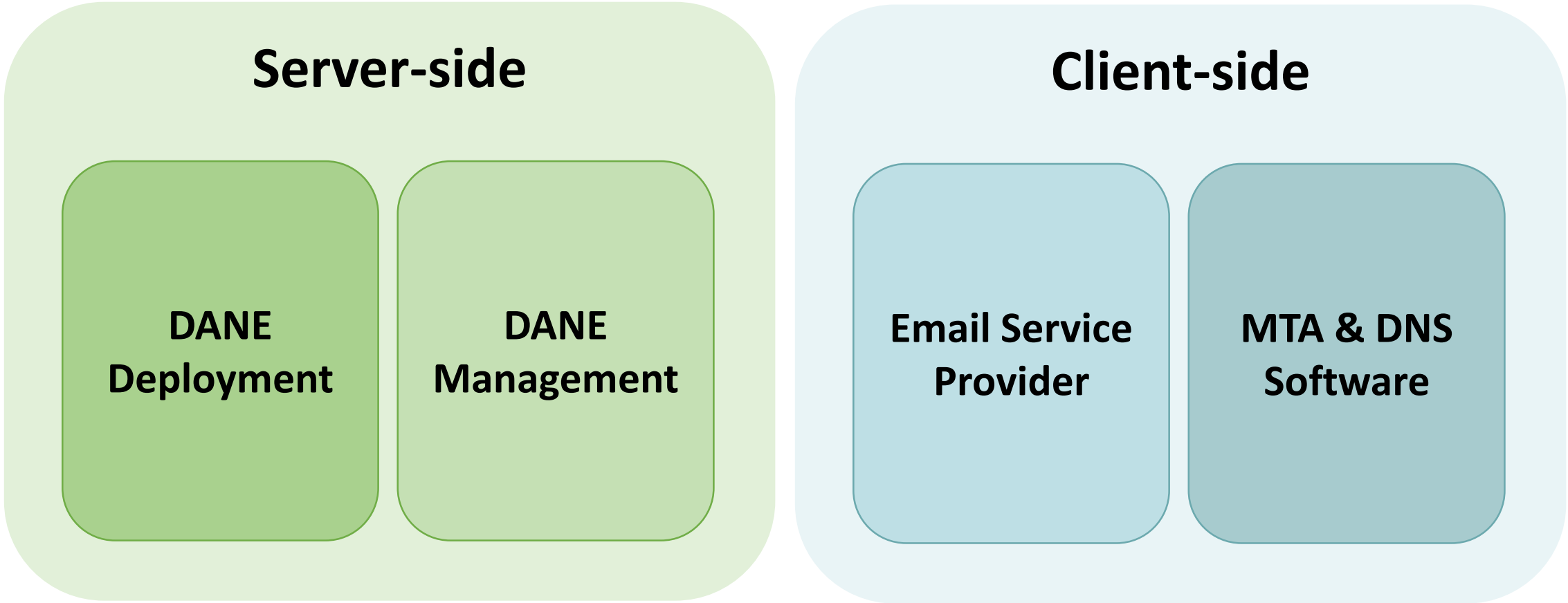
- Support **STARTTLS**

Analysis

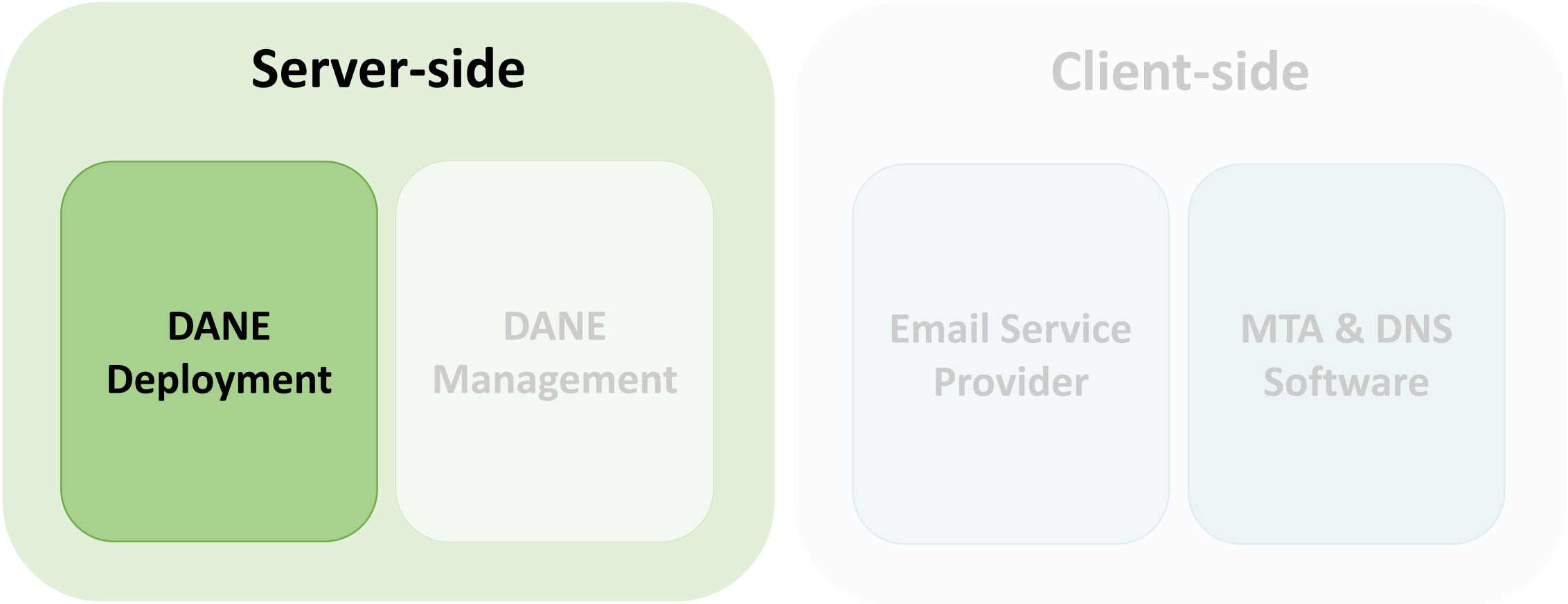
Deployment
TLSA
2 years Every Day
5 TLD* *.com, .net, .org* *.se, .nl*
Management
TLSA Certificate
4 months Every Hour

*OpenINTEL (https://openintel.nl/)

Outline of Analysis

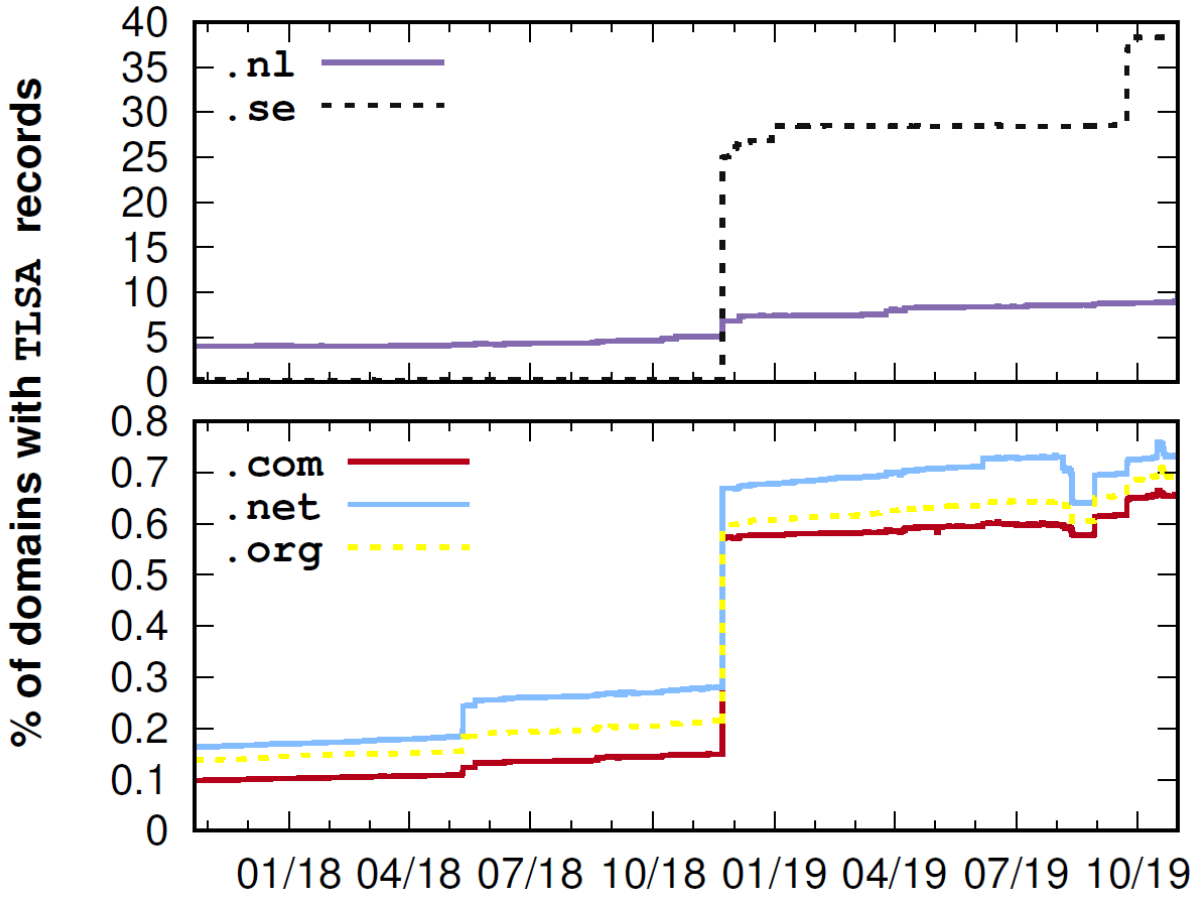


Outline of Analysis



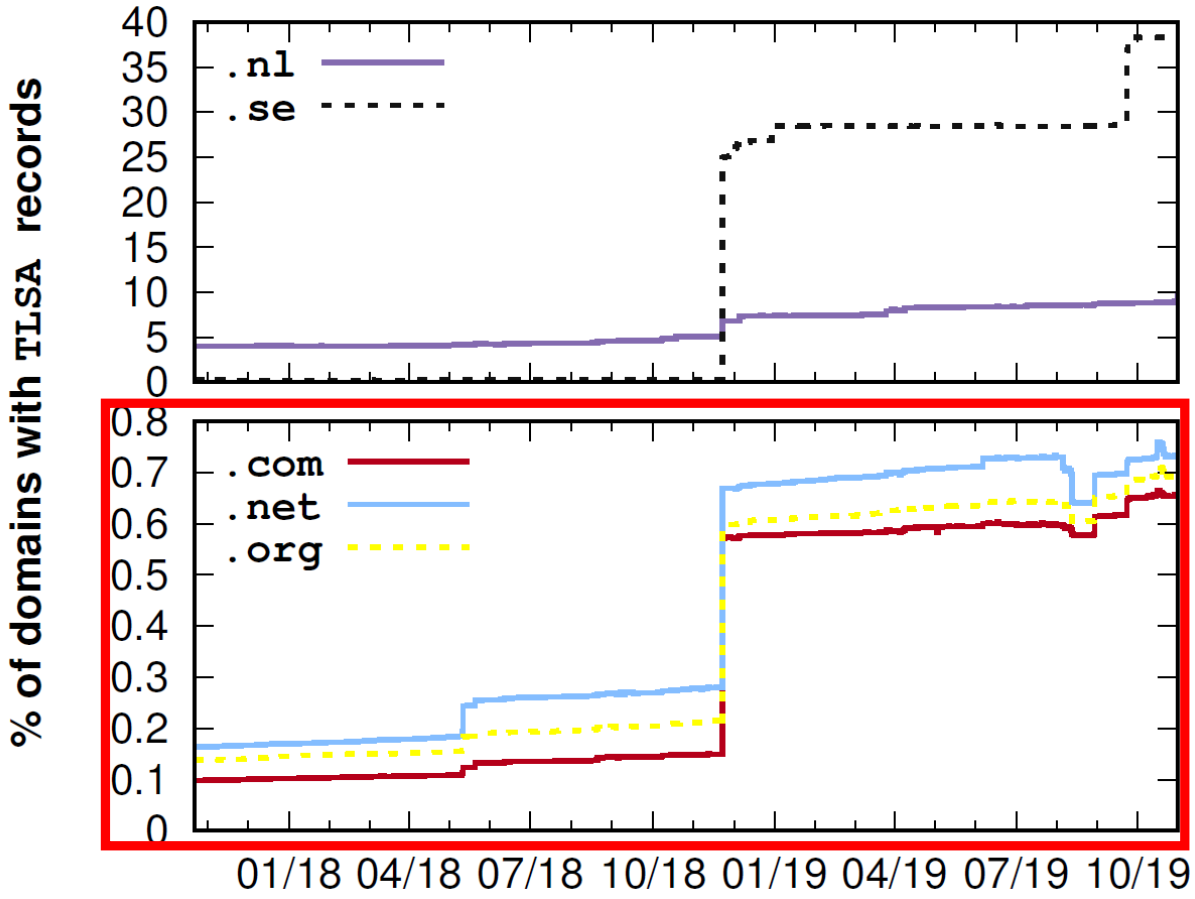
DANE Deployment

- Deployment is rare, but steadily growing



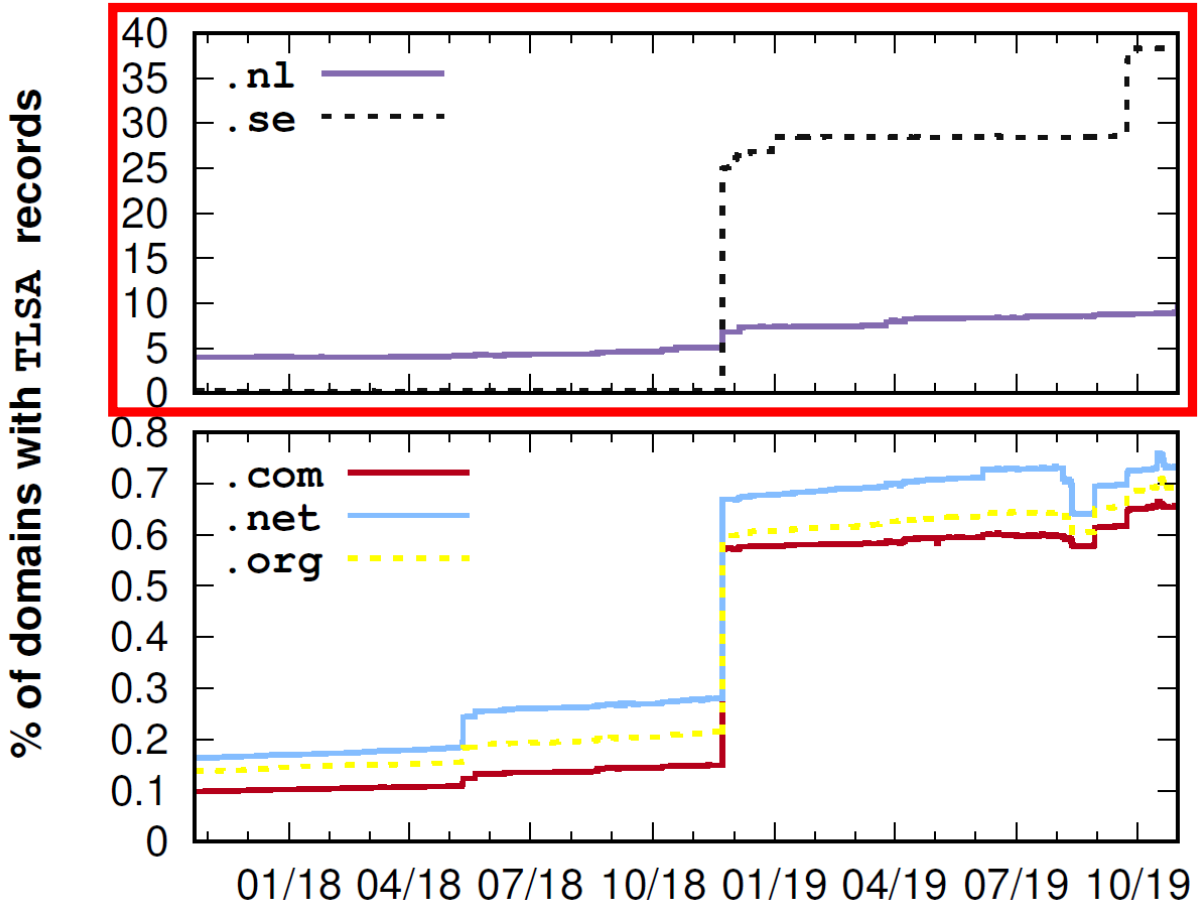
DANE Deployment

- Deployment is rare, but steadily growing



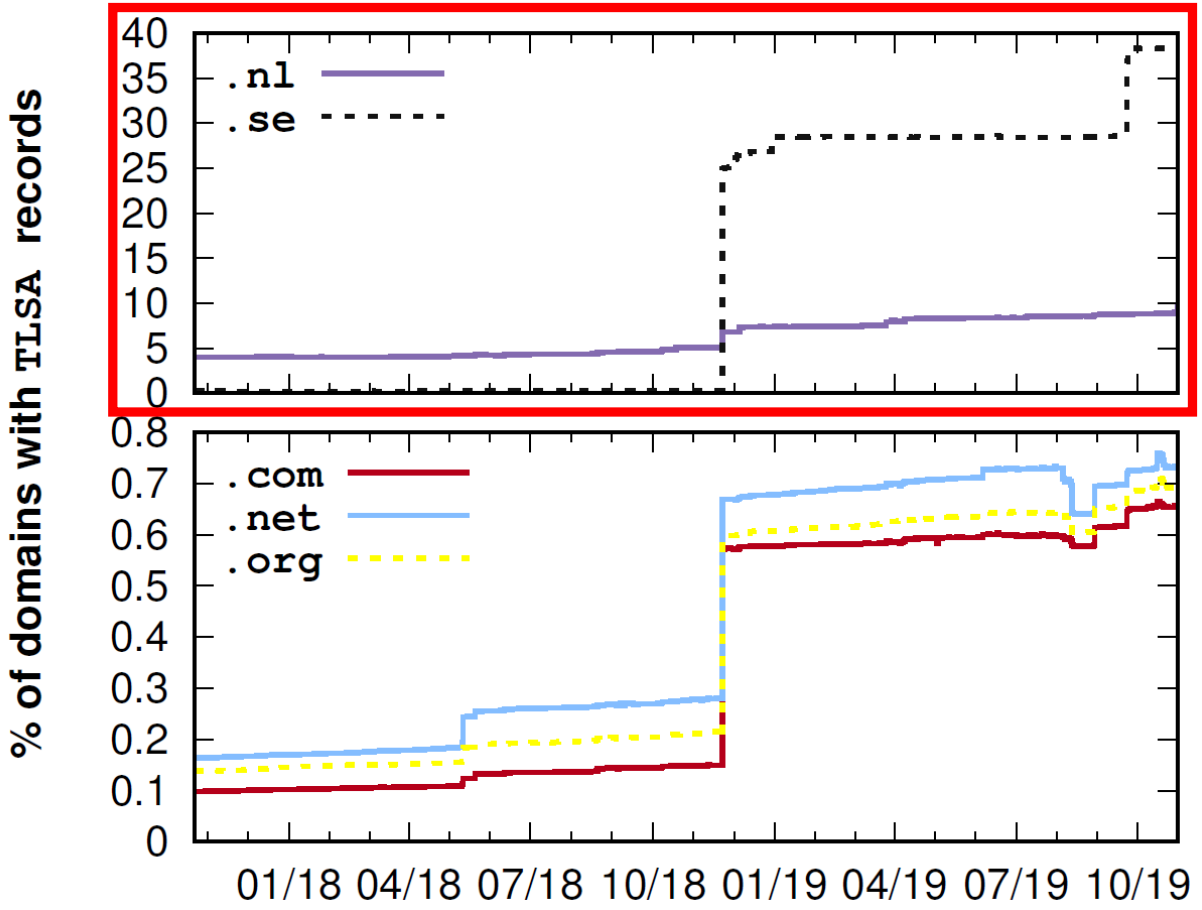
DANE Deployment

- Deployment is rare, but steadily growing
- The deployment rate for .nl and .se is high



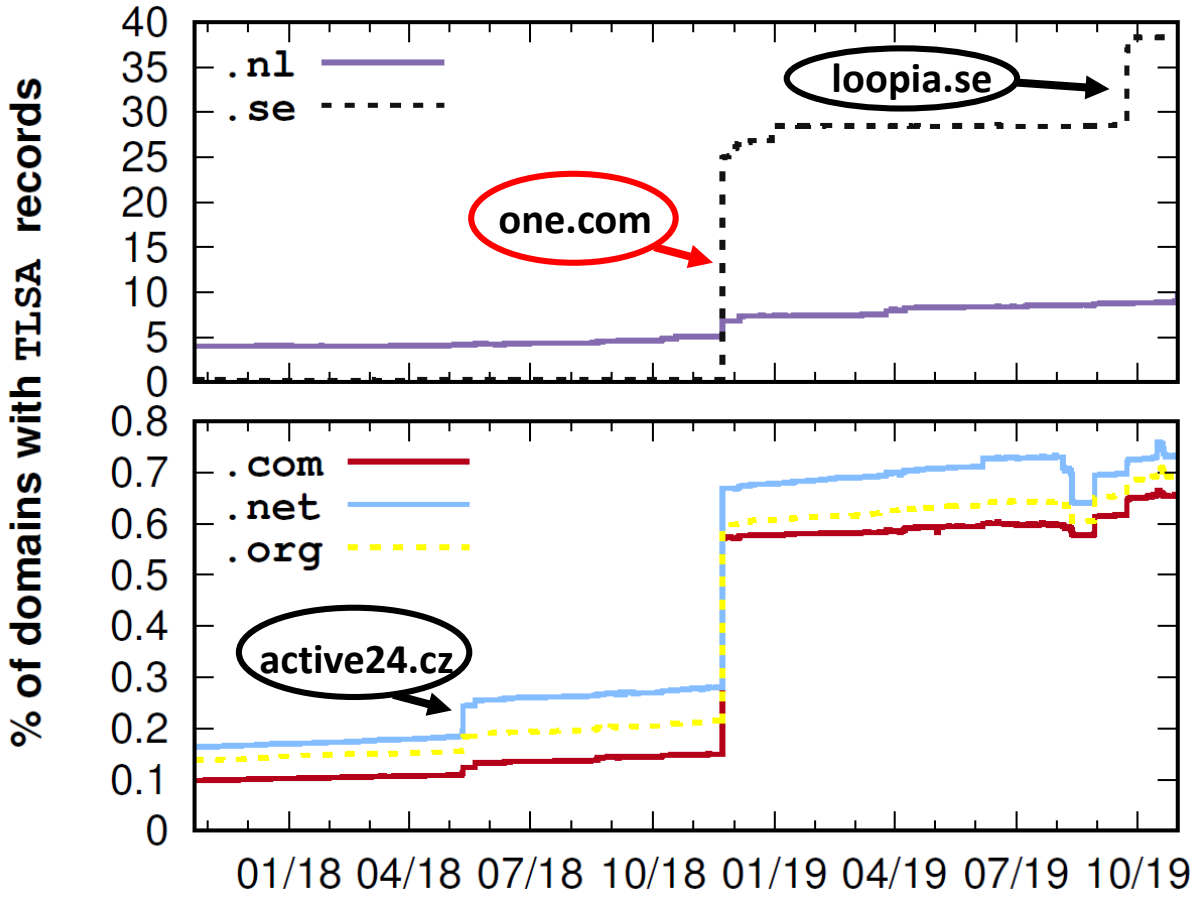
DANE Deployment

- Deployment is rare, but steadily growing
- The deployment rate for .nl and .se is high
  → Financial incentives from registries



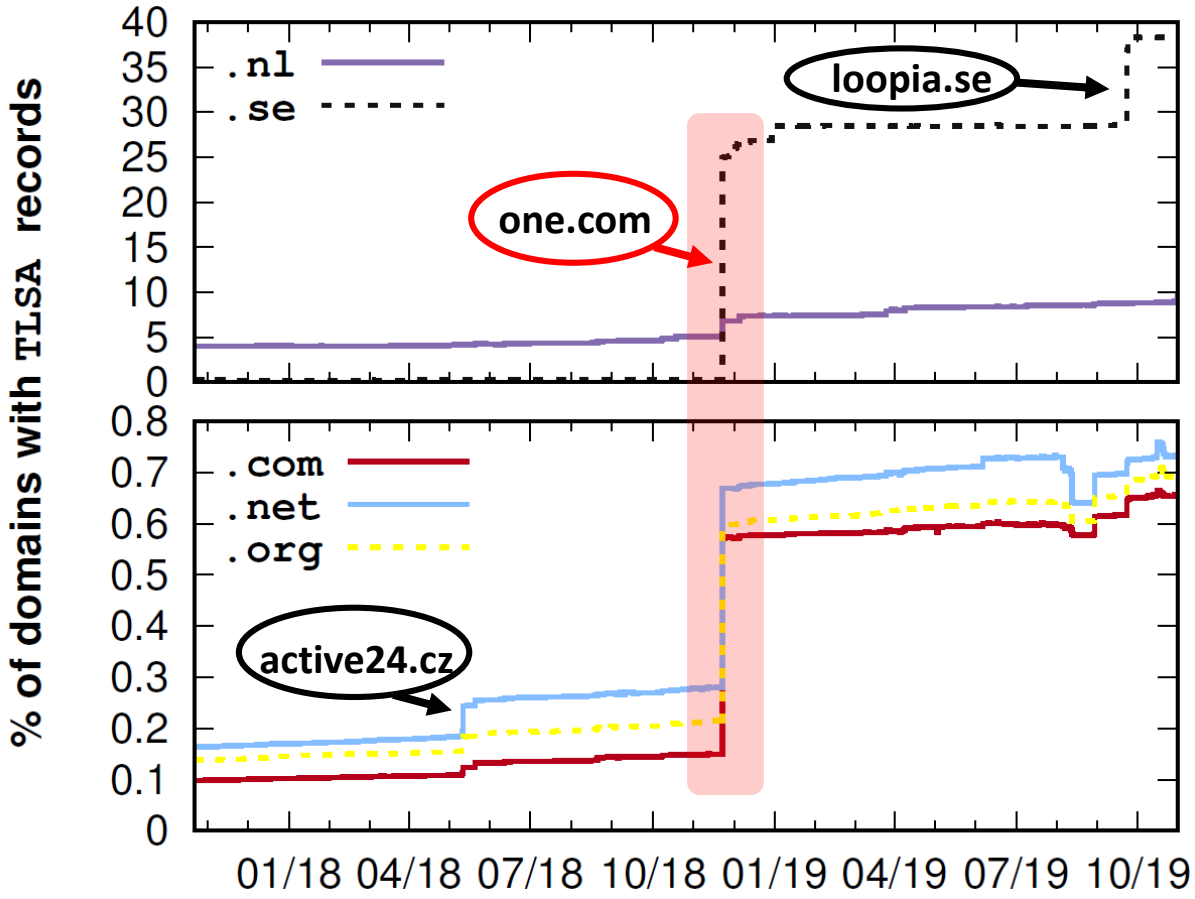
DANE Deployment

- Deployment is rare, but steadily growing
- The deployment rate for .nl and .se is high
  → Financial incentives from registries
- Growth is mainly due to a small number of popular email service providers



DANE Deployment

- Deployment is rare, but steadily growing
- The deployment rate for .nl and .se is high
  → Financial incentives from registries
- Growth is mainly due to a small number of popular email service providers



DANE Deployment – Summary

DANE deployment is growing

0.6~0.7% (.com, .net, .org) 10% (.nl) 37% (.se)

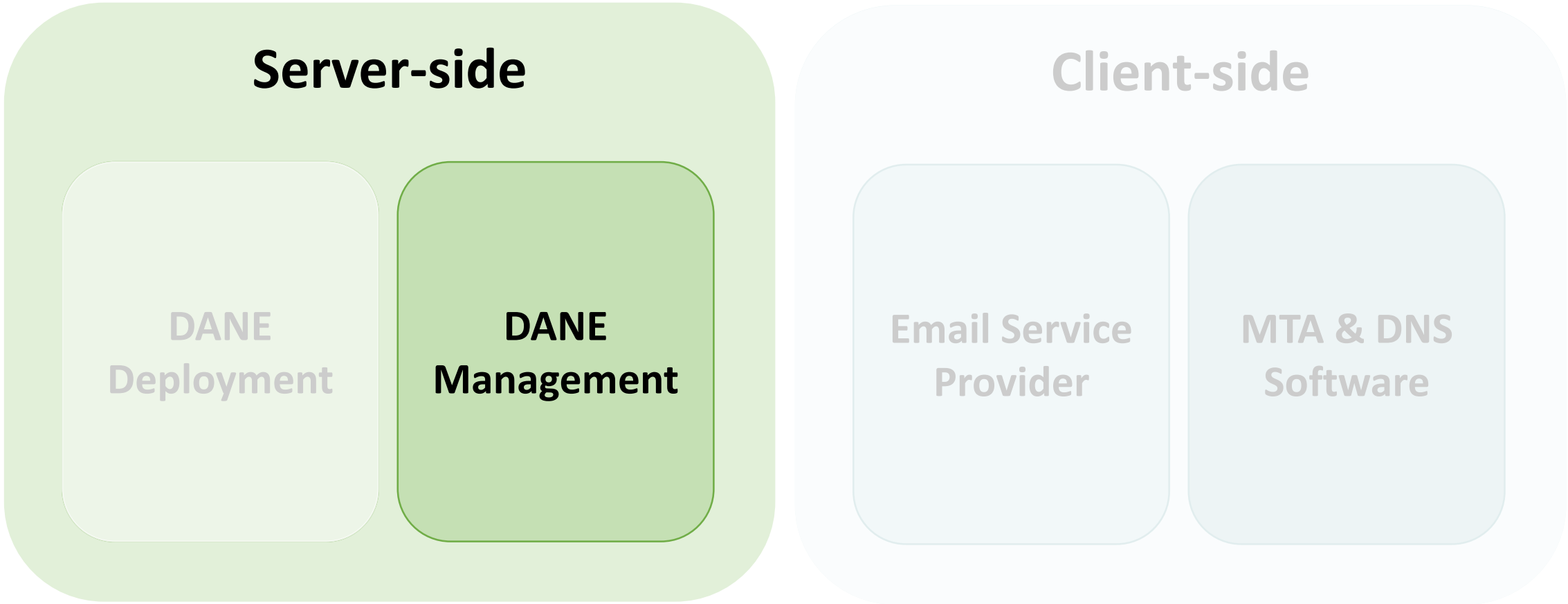
DANE Deployment – Summary

DANE deployment is growing

0.6~0.7% (.com, .net, .org) 10% (.nl) 37% (.se)

Are they deployed DANE correctly?

Outline of Analysis



Condition for Correct DANE Management

Support?

- **DS & RRSIG** records are published

DNSSEC

Condition for Correct DANE Management

Support?

- **DS & RRSIG** records are published — **DNSSEC**
- **Certificates** are provided — **STARTTLS**

Condition for Correct DANE Management

Support?		Correctly?
- **DS & RRSIG** records are published	**DNSSEC**	- DNSSEC records are **correct** (e.g. not expired)
- **Certificates** are provided	**STARTTLS**	- Certificates are **consistent** with TLSA records

Condition for Correct DANE Management

Support?		Correctly?
- DS & RRSIG records are published	DNSSEC	- RRSIG records are correct (e.g. not expired)
Missing Components		**Incorrect Components**
- Certificates are provided	STARTTLS	- Certificates match with TLSA records

Condition for Correct DANE Management

Support?

Correctly?

- DS & RRSIG records are published
- Certificates are provided

Missing Components

DNSSEC

STARTTLS

- RRSIG records are correct (e.g. not expired)
- Certificates match with TLSA records

Incorrect Components

4 months / every hour

5 vantage points (Oregon, Virginia, São Paulo, Paris, Sydney)

Condition for Correct DANE Management

Support?

Correctly?

- DS & RRSIG records are published
- Certificates are provided

Missing Components

DNSSEC

STARTTLS

- RRSIG records are correct (e.g. not expired)
- Certificates match with TLSA records

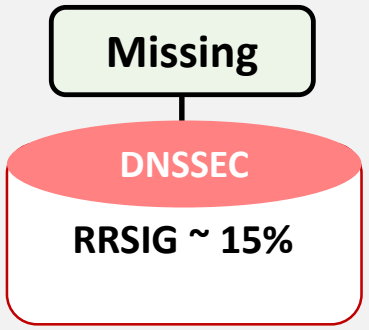
Incorrect Components

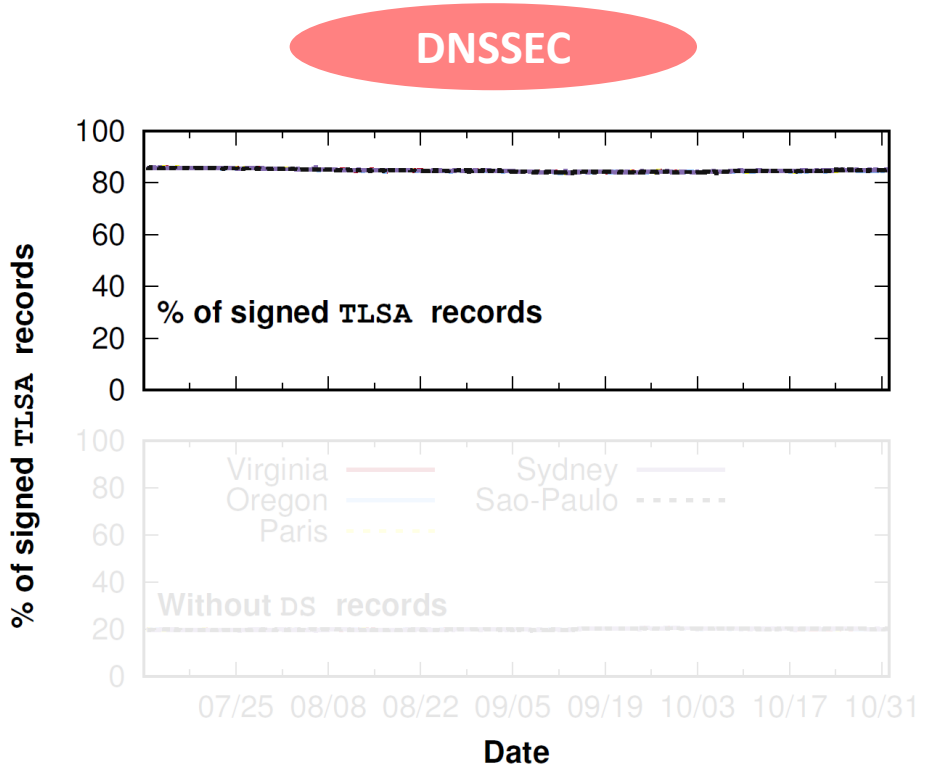
4 months / every hour

5 vantage points (Oregon, Virginia, São Paulo, Paris, Sydney)

→ No difference

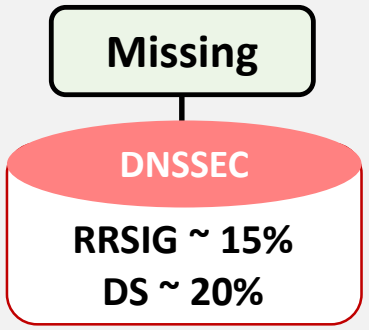
Missing Components

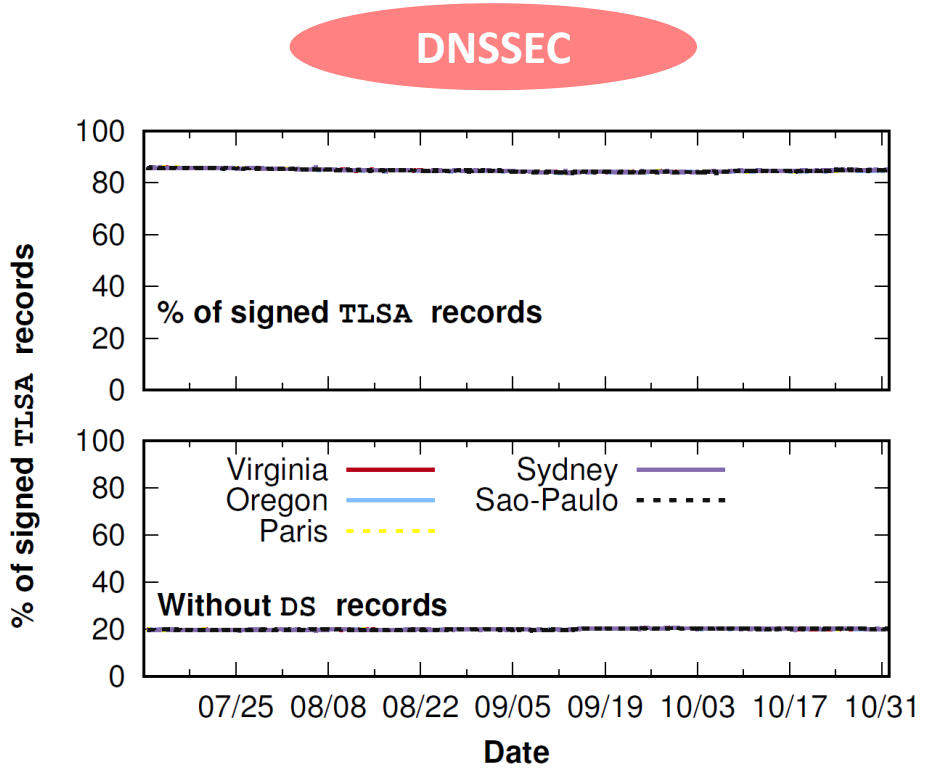




85% are signed (have **RRSIG record**)

Missing Components





85% are signed (have **RRSIG record**)

20% of them do not have **DS records**

Missing Components

Missing

DNSSEC

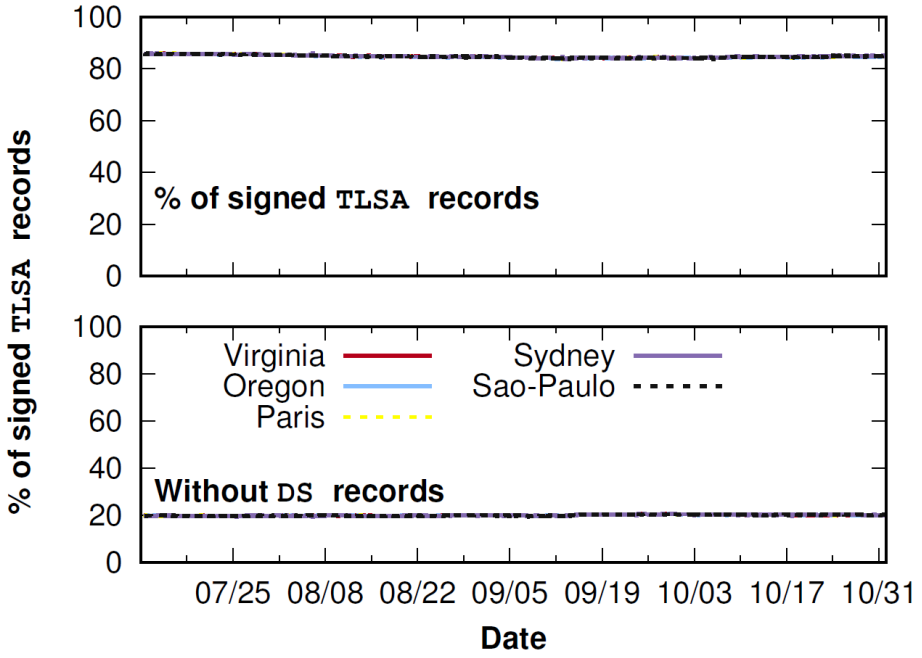
RRSIG ~ 15%

DS ~ 20%

STARTTLS

STARTTLS ~ 0.3%

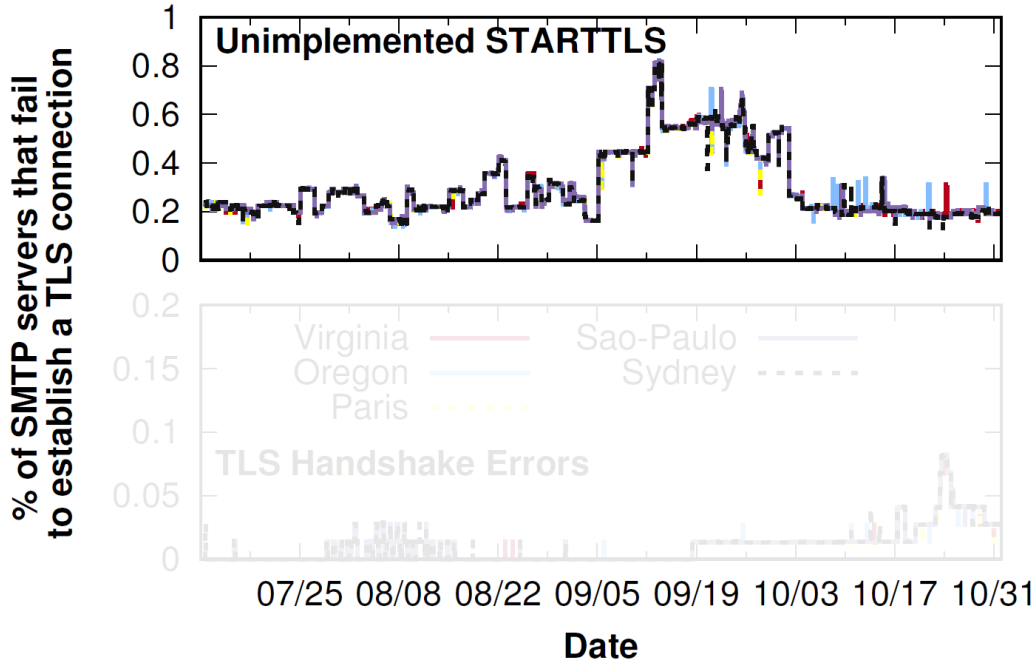
DNSSEC



85% are signed (have **RRSIG record**)

20% of them do not have **DS records**

STARTTLS



99.7% supports **STARTTLS**

Missing Components

Missing

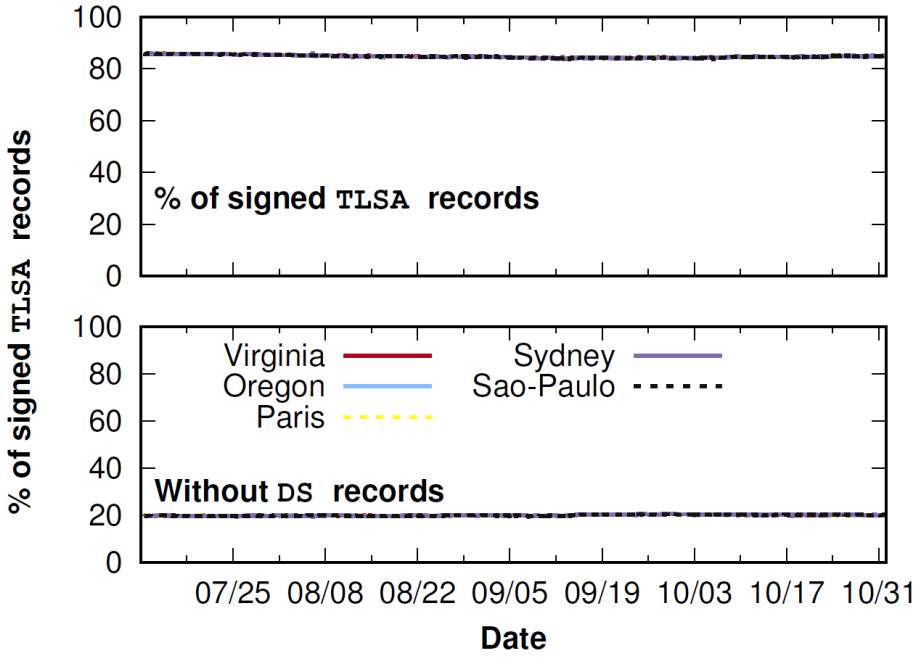
DNSSEC

RRSIG ~ 15%
DS ~ 20%

STARTTLS

STARTTLS ~ 0.3%
Certificate ~ 0.01%

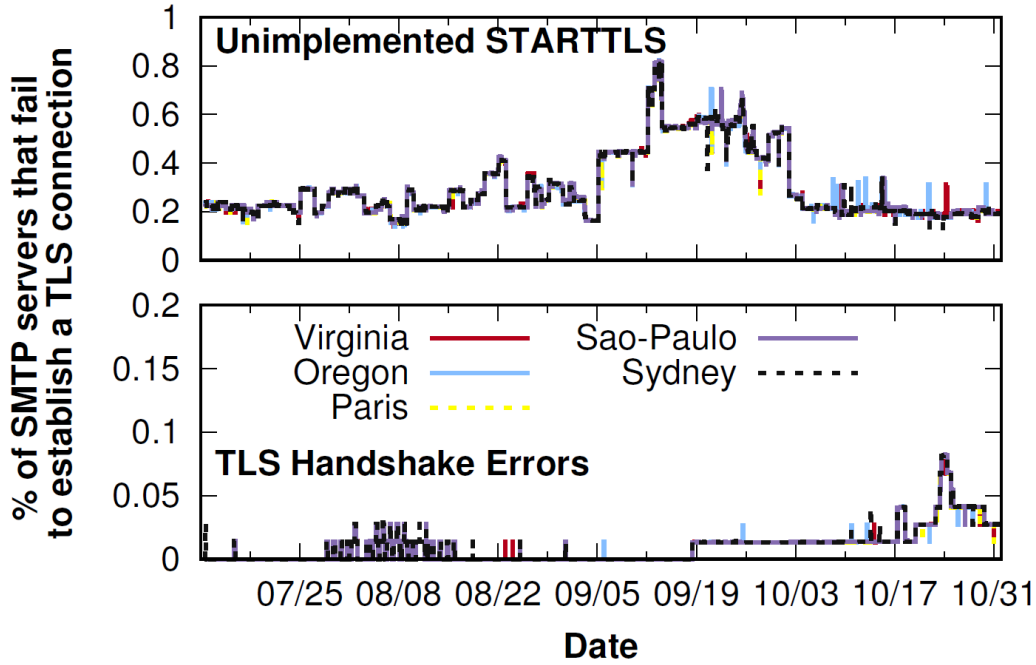
DNSSEC



85% are signed (have **RRSIG record**)

20% of them do not have **DS records**

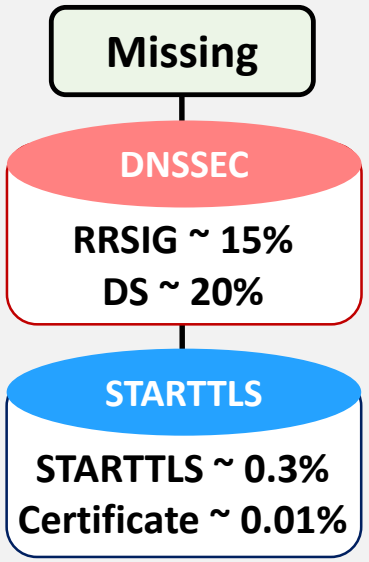
STARTTLS



99.7% supports **STARTTLS**

0.01% of them provide no or malformed **certificates**

Missing Components



Main failure reason?

Missing DS records

rather than the absence of STARTTLS support

Incorrect Components

Missing

DNSSEC

RRSIG ~ 15%
DS ~ 20%

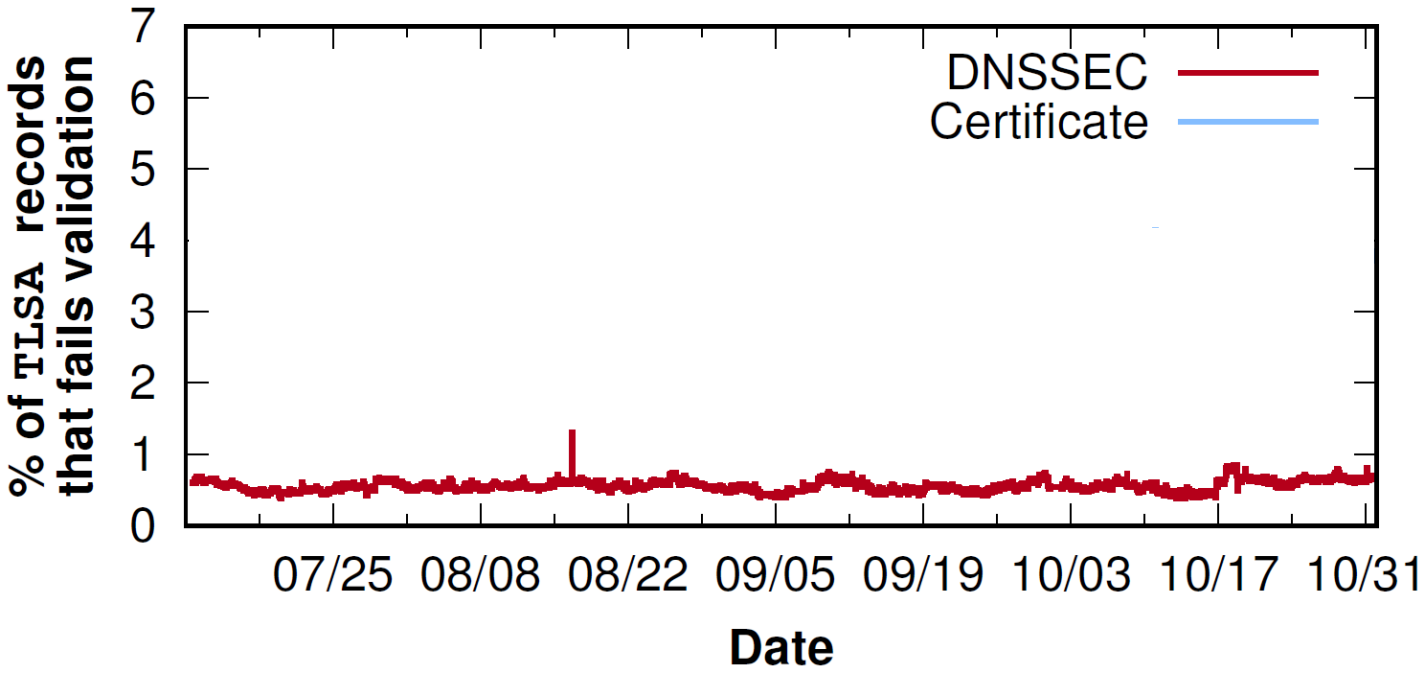
STARTTLS

STARTTLS ~ 0.3%
Certificate ~ 0.01%

Incorrect

DNSSEC

Validation fail
~ 0.55%



DNSSEC **0.55%** of DNSSEC records are **incorrect**

Incorrect Components

Missing

DNSSEC

RRSIG ~ 15%
DS ~ 20%

STARTTLS

STARTTLS ~ 0.3%
Certificate ~ 0.01%

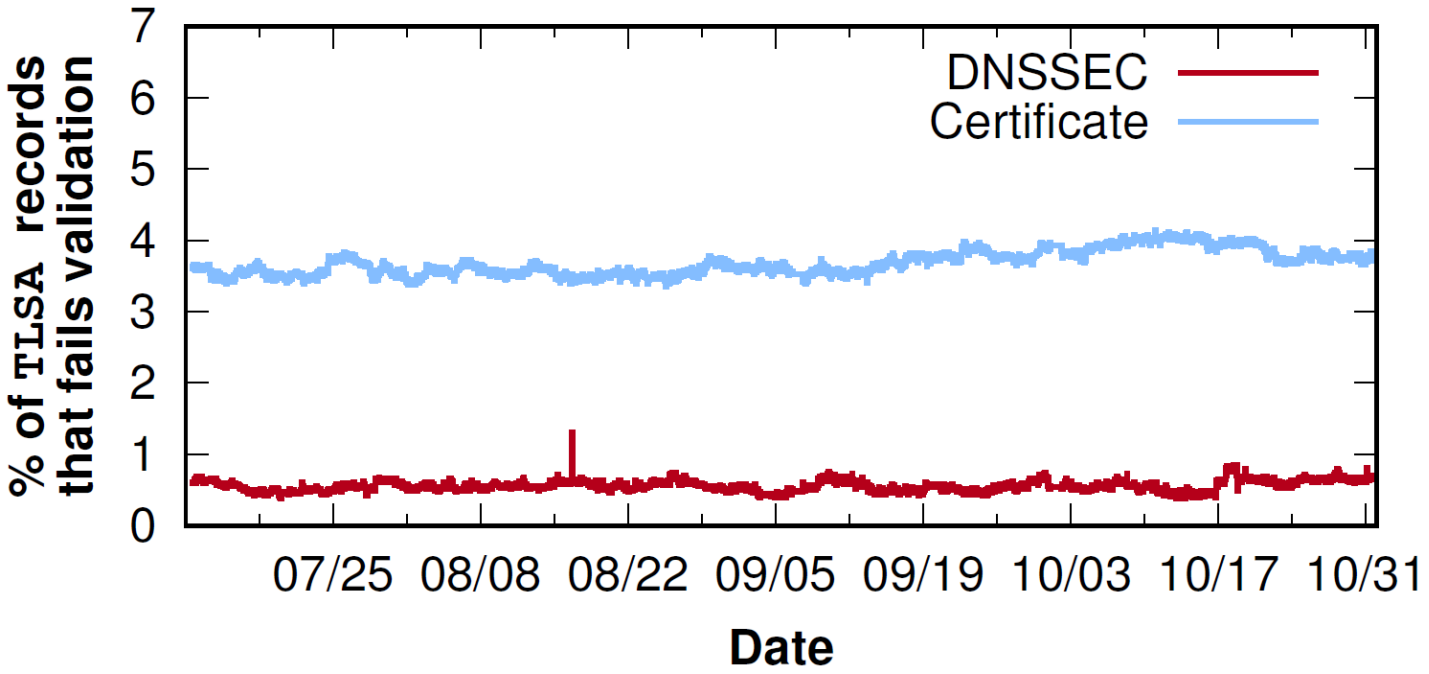
Incorrect

DNSSEC

Validation fail
~ 0.55%

STARTTLS

Mismatch ~ 3.68%



DNSSEC **0.55%** of DNSSEC records are **incorrect**

STARTTLS **3.68%** of certificates do **not match** with their corresponding TLSA records

DANE Management – Summary

Mismanagement in the DANE ecosystem is pervasive

Missing or incorrect DNSSEC - 35%

Outline of Analysis

Server-side

DANE Deployment

DANE Management

Client-side

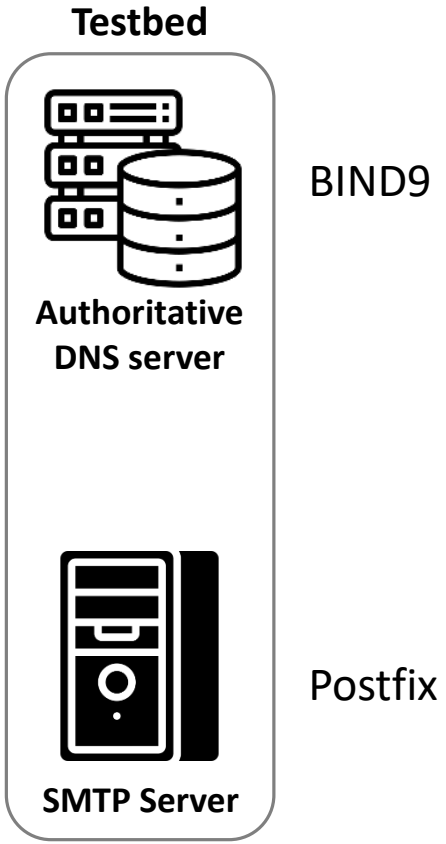
Email Service Provider

MTA & DNS Software

Popular Email Service Providers

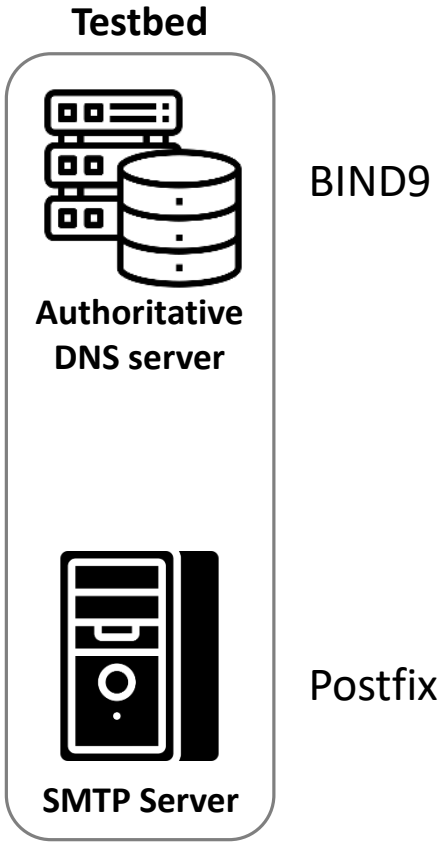
How many popular email service providers do support DANE and correctly?

Testbed


Testbed
Authoritative
DNS server
BIND9
SMTP Server
Postfix

Testbed

- Purchase a second-level domain name
  ex) *dane-test.com*

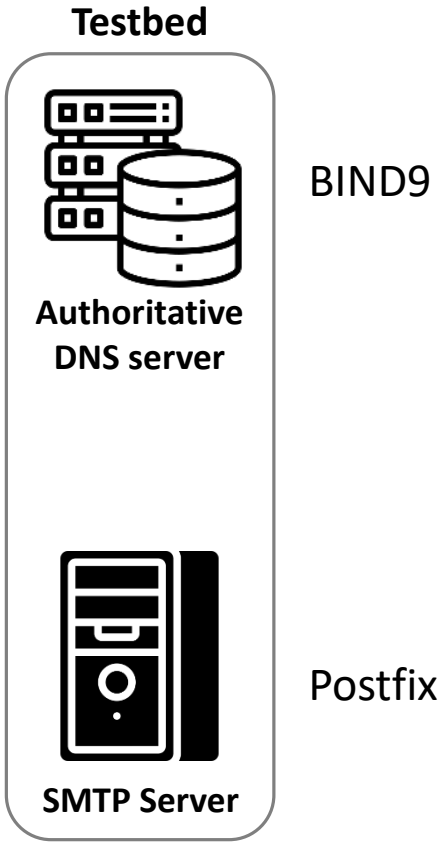


Testbed

- Purchase a second-level domain name
  ex) *dane-test.com*

- Set subdomains that are configured to different combination of DNSSEC, STARTTLS, and DANE misconfigurations

  ex) *dnssec-expired-rrsig.dane-test.com*
  cert-tlsa-unmatched.dane-test.com



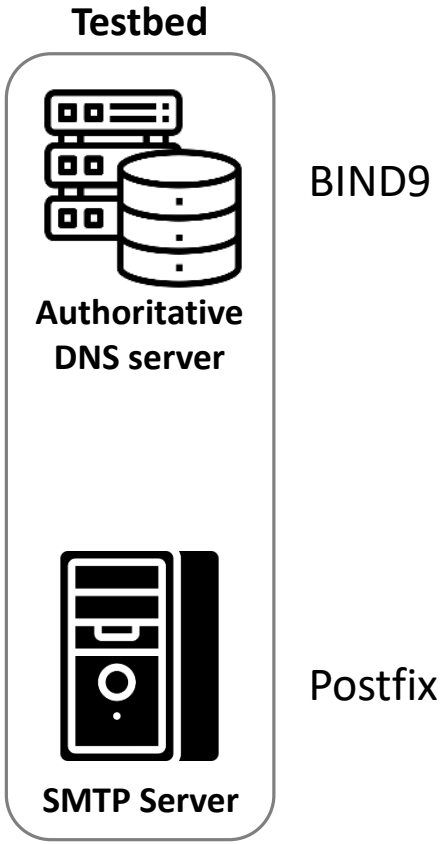
Testbed

- Purchase a second-level domain name
  ex) *dane-test.com*

- Set subdomains that are configured to different combination of DNSSEC, STARTTLS, and DANE misconfigurations

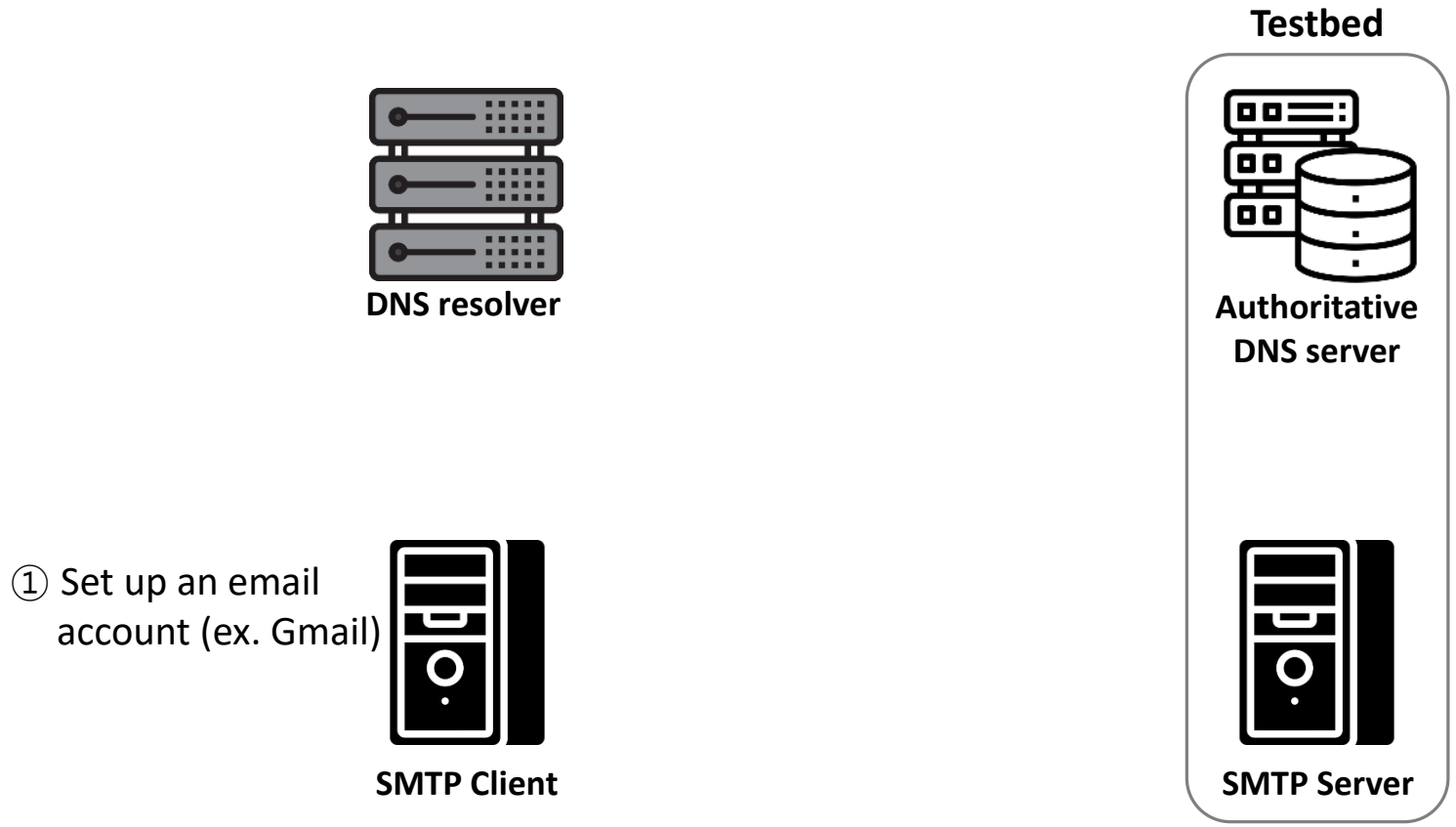
  ex) *dnssec-expired-rrsig.dane-test.com*
  cert-tlsa-unmatched.dane-test.com

**Test 29 popular*
email service providers**

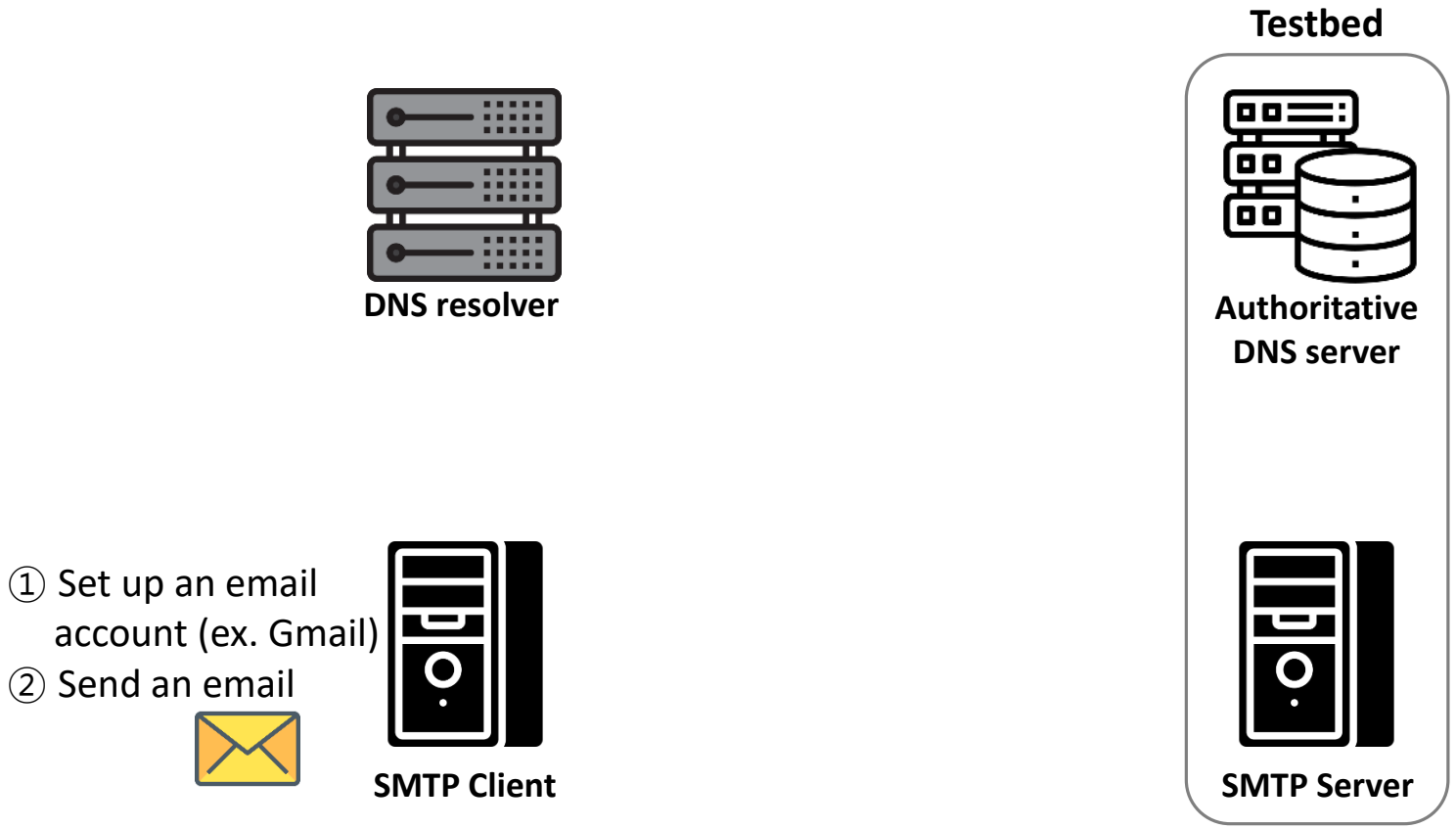


*Rank from Adobe's leaked user email database (2013)

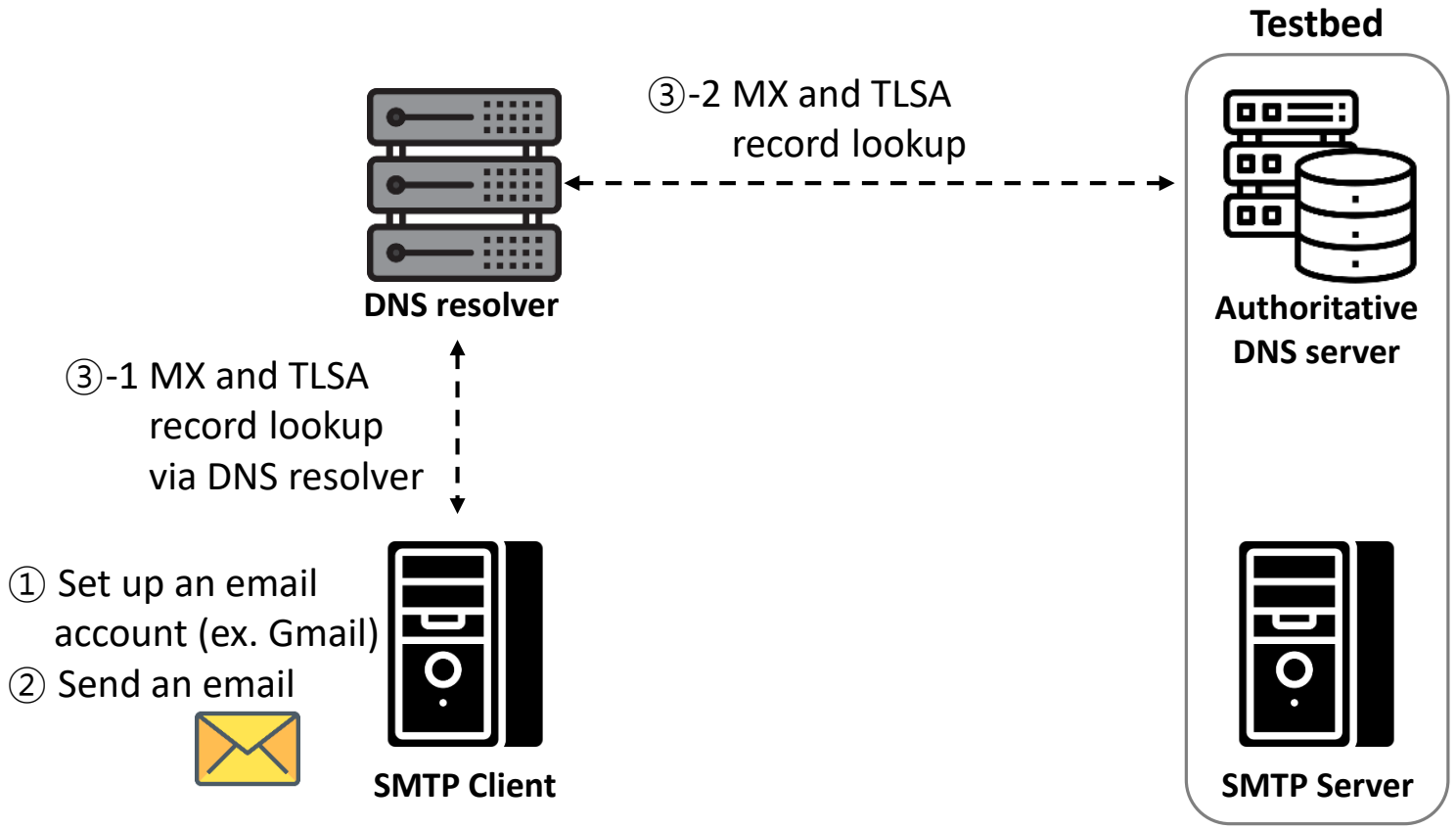
Testbed


Testbed
DNS resolver
Authoritative
DNS server
① Set up an email
account (ex. Gmail)
SMTP Client
SMTP Server

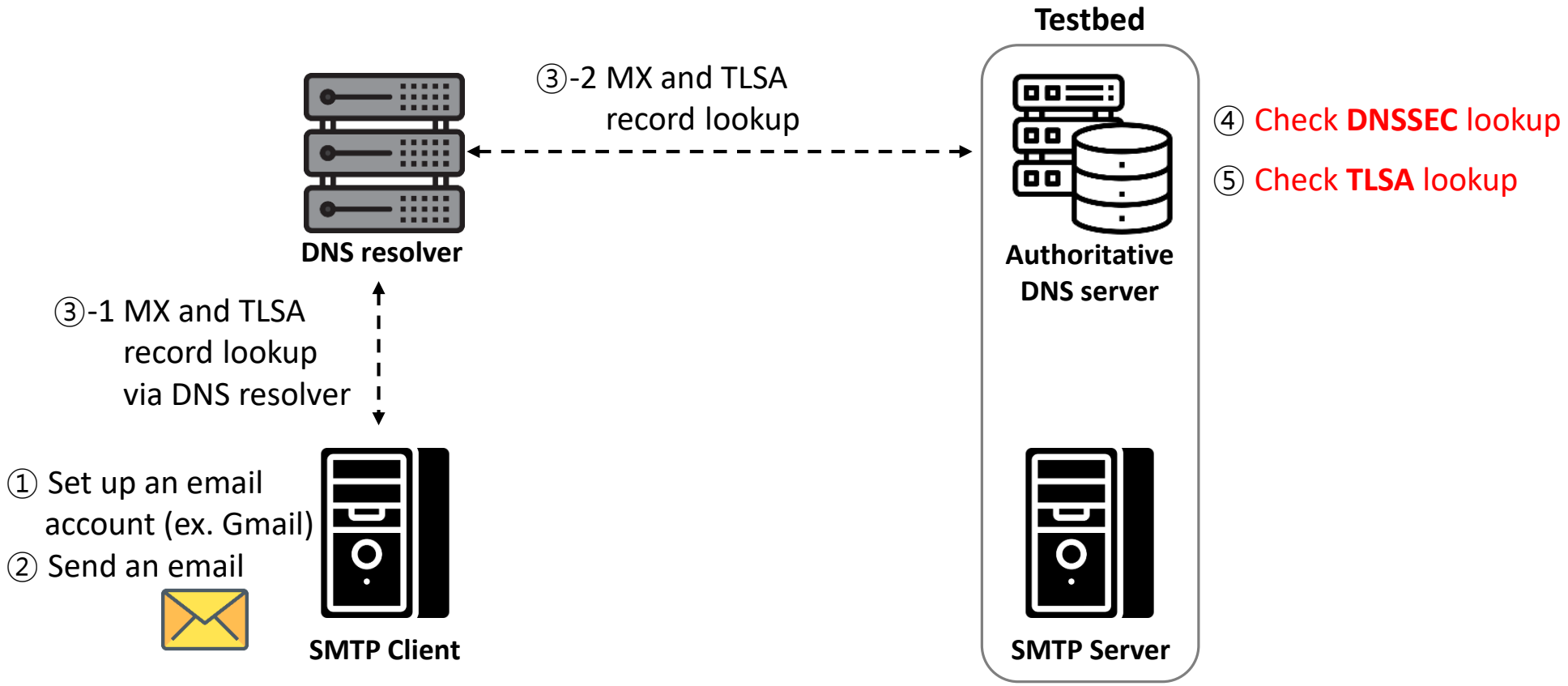
Testbed


Testbed
DNS resolver
Authoritative
DNS server
① Set up an email
account (ex. Gmail)
② Send an email
SMTP Client
SMTP Server

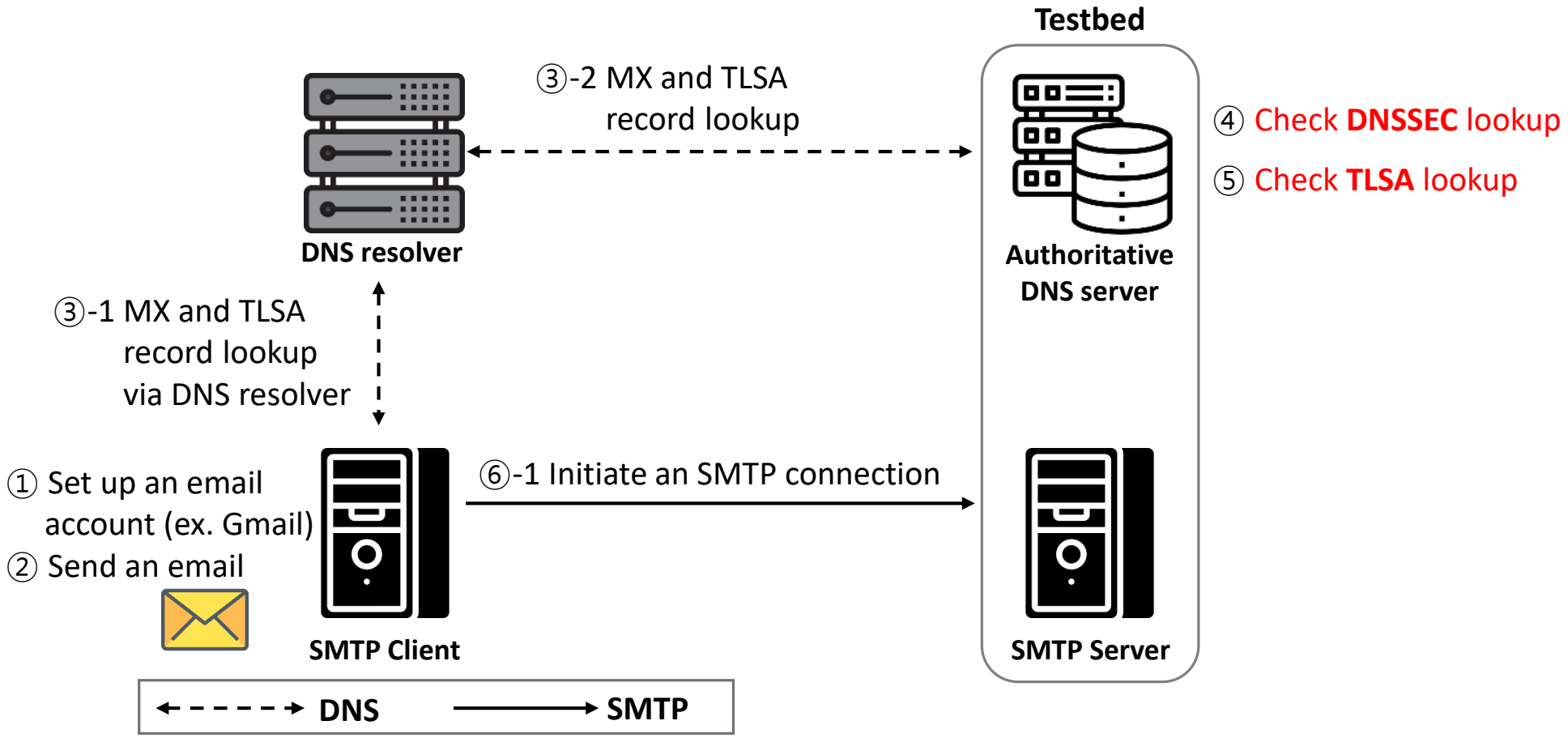
Testbed


Testbed
③-2 MX and TLSA
record lookup
DNS resolver
Authoritative
DNS server
③-1 MX and TLSA
record lookup
via DNS resolver
① Set up an email
account (ex. Gmail)
② Send an email
SMTP Client
SMTP Server

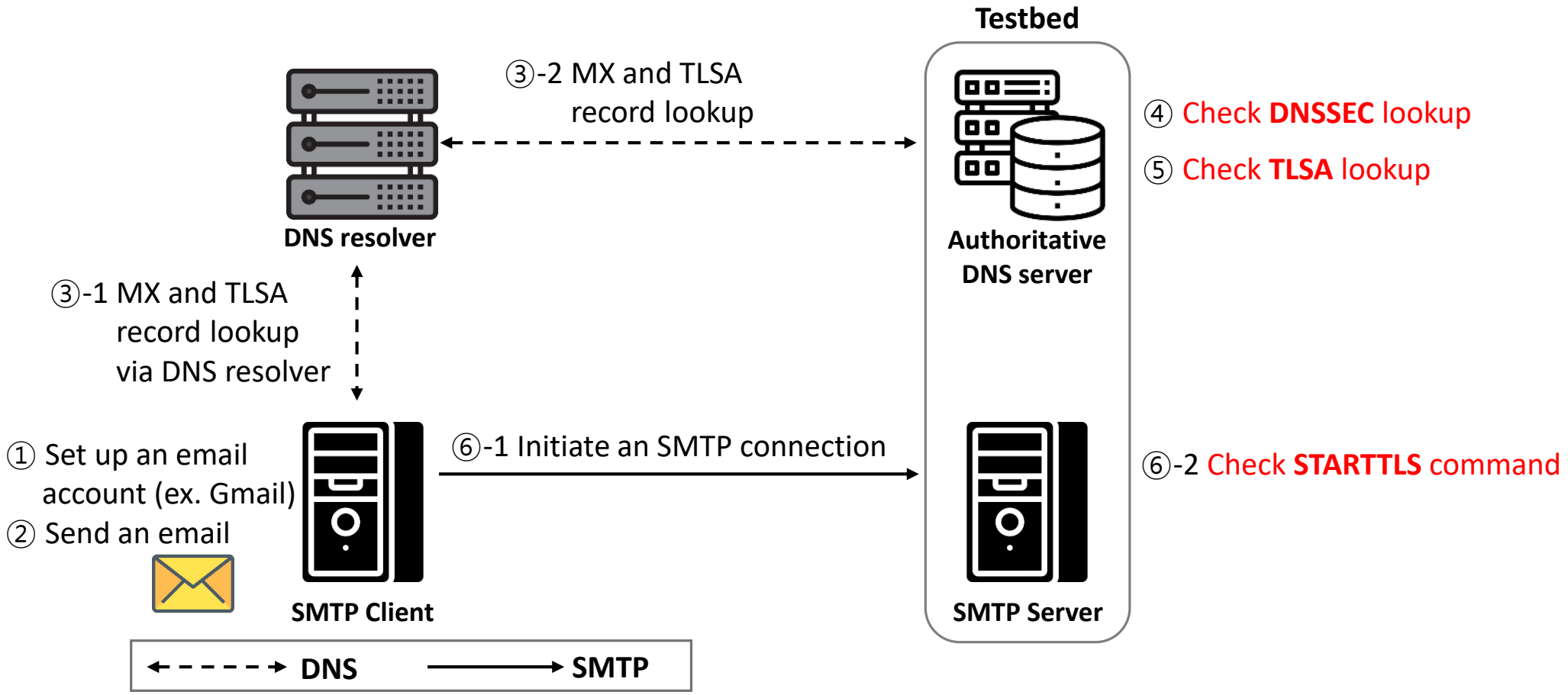
Testbed


Testbed
③-2 MX and TLSA
record lookup
DNS resolver
Authoritative
DNS server
④ Check DNSSEC lookup
⑤ Check TLSA lookup
③-1 MX and TLSA
record lookup
via DNS resolver
① Set up an email
account (ex. Gmail)
② Send an email
SMTP Client
SMTP Server

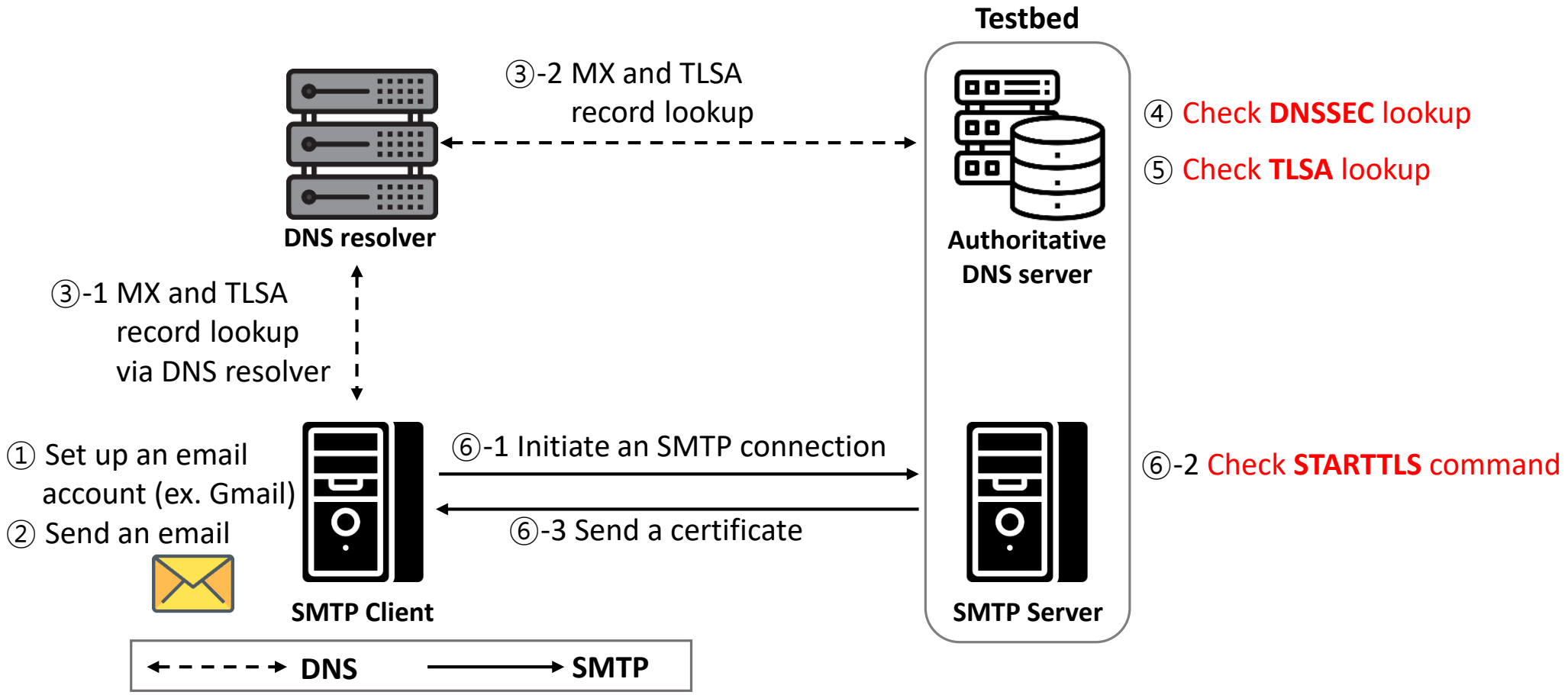
Testbed


Testbed
③-2 MX and TLSA
record lookup
④ Check DNSSEC lookup
⑤ Check TLSA lookup
DNS resolver
Authoritative
DNS server
③-1 MX and TLSA
record lookup
via DNS resolver
① Set up an email
account (ex. Gmail)
② Send an email
⑥-1 Initiate an SMTP connection
SMTP Client
SMTP Server
DNS
SMTP

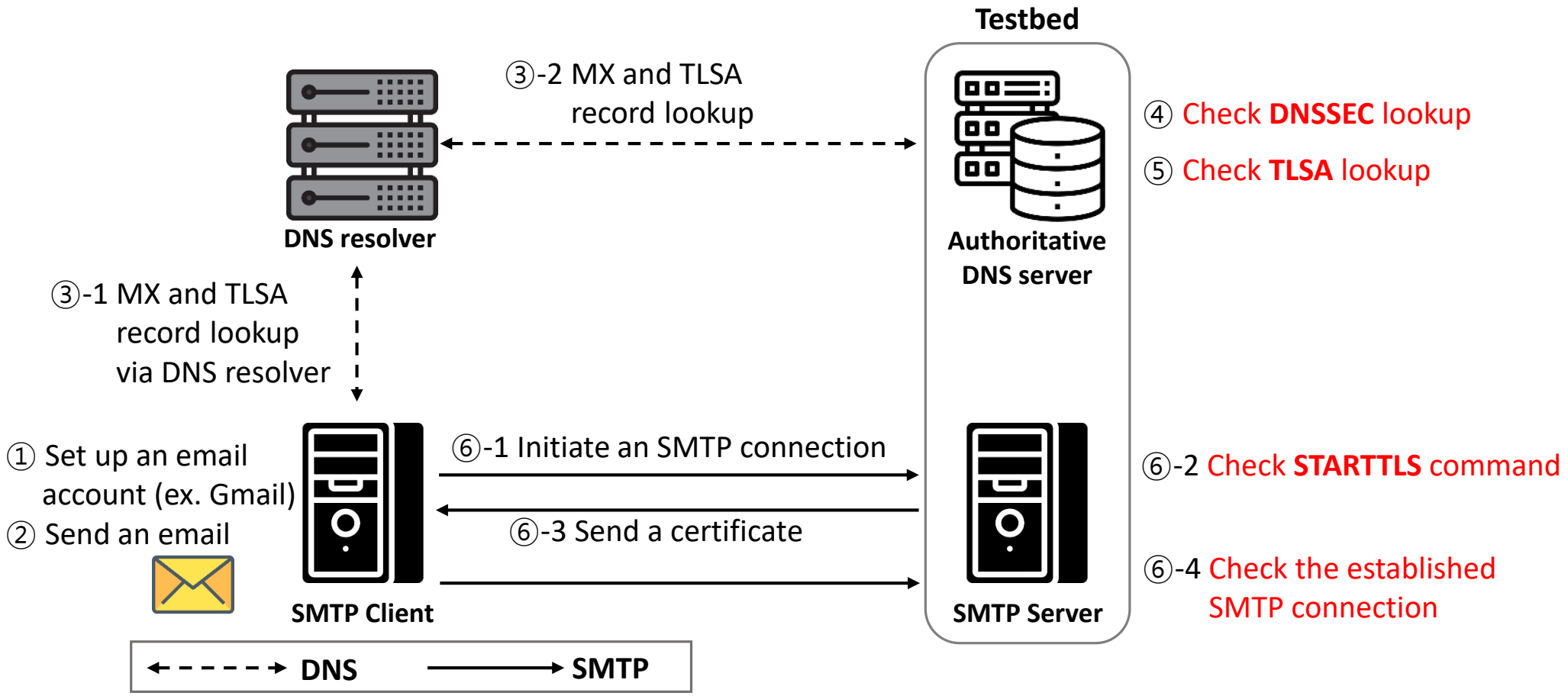
Testbed


Testbed
③-2 MX and TLSA
record lookup
DNS resolver
Authoritative
DNS server
④ Check DNSSEC lookup
⑤ Check TLSA lookup
③-1 MX and TLSA
record lookup
via DNS resolver
① Set up an email
account (ex. Gmail)
② Send an email
⑥-1 Initiate an SMTP connection
SMTP Client
SMTP Server
⑥-2 Check STARTTLS command
DNS
SMTP

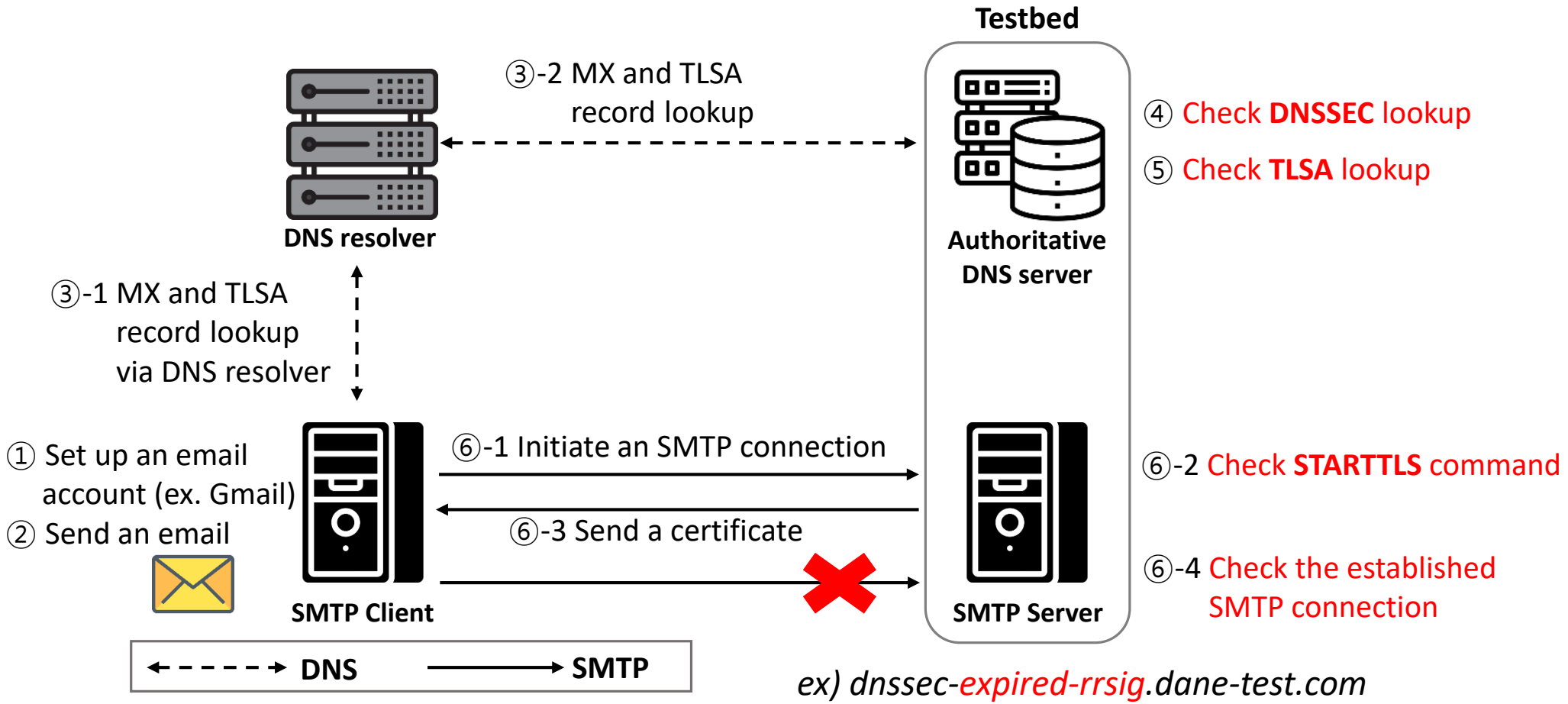
Testbed


Testbed
③-2 MX and TLSA record lookup
DNS resolver
Authoritative DNS server
④ Check DNSSEC lookup
⑤ Check TLSA lookup
③-1 MX and TLSA record lookup via DNS resolver
① Set up an email account (ex. Gmail)
② Send an email
⑥-1 Initiate an SMTP connection
⑥-3 Send a certificate
⑥-2 Check STARTTLS command
SMTP Client
SMTP Server
DNS
SMTP

Testbed


Testbed
③-2 MX and TLSA record lookup
DNS resolver
Authoritative DNS server
④ Check DNSSEC lookup
⑤ Check TLSA lookup
③-1 MX and TLSA record lookup via DNS resolver
① Set up an email account (ex. Gmail)
② Send an email
⑥-1 Initiate an SMTP connection
⑥-3 Send a certificate
SMTP Client
SMTP Server
⑥-2 Check STARTTLS command
⑥-4 Check the established SMTP connection
DNS
SMTP

Testbed


Testbed
③-2 MX and TLSA record lookup
DNS resolver
Authoritative DNS server
④ Check DNSSEC lookup
⑤ Check TLSA lookup
③-1 MX and TLSA record lookup via DNS resolver
① Set up an email account (ex. Gmail)
② Send an email
⑥-1 Initiate an SMTP connection
⑥-3 Send a certificate
SMTP Client
SMTP Server
⑥-2 Check STARTTLS command
⑥-4 Check the established SMTP connection
DNS
SMTP
ex) dnssec-expired-rrsig.dane-test.com

Popular Email Service Providers' DANE Support

Total 29

Mail Provider	DNSSEC Request (DNSKEY, DS)	Validation
mail.com	✓	✓
comcast.net	✓	✓
gmx.com	✓	✓
tutanota.com	✓	✓
mynet.com	✓	×
sapo.pt	✓	×
sina.com	✓	×
protonmail.com	×	×
aol.com	×	×
fastmail.com	×	×
freemail.hu	×	×
mail.ru	×	×
naver.com	×	×
rediffmail.com	×	×
yahoo.com	×	×
zoho.in	×	×
daum.net	×	×
interia.pl	×	×
inbox.lv	×	×
icloud.com	×	×
runbox.com	×	×
seznam.cz	×	×
o2.pl	×	×
wp.pl	×	×
sohu.com	×	×
t-online.de	×	×
excite.com	×	×
gmail.com	×	×
outlook.com	×	×

DNSSEC

- Only 7 email providers actually fetch DNSKEY and DS records

Popular Email Service Providers' DANE Support

Total 29

Mail Provider	DNSSEC Request (DNSKEY, DS)	Validation
mail.com	✓	✓
comcast.net	✓	✓
gmx.com	✓	✓
tutanota.com	✓	✓
mynet.com	✓	×
sapo.pt	✓	×
sina.com	✓	×
protonmail.com	×	×
aol.com	×	×
fastmail.com	×	×
freemail.hu	×	×
mail.ru	×	×
naver.com	×	×
rediffmail.com	×	×
yahoo.com	×	×
zoho.in	×	×
daum.net	×	×
interia.pl	×	×
inbox.lv	×	×
icloud.com	×	×
runbox.com	×	×
seznam.cz	×	×
o2.pl	×	×
wp.pl	×	×
sohu.com	×	×
t-online.de	×	×
excite.com	×	×
gmail.com	×	×
outlook.com	×	×

DNSSEC

- Only 7 email providers actually fetch DNSKEY and DS records
- Only 4 providers correctly verify DNSSEC records

Popular Email Service Providers' DANE Support

Total 29

Mail Provider	STARTTLS Support
mail.com	✓
comcast.net	✓
gmx.com	✓
tutanota.com	✓
mynet.com	✓
sapo.pt	✓
sina.com	×
protonmail.com	✓
aol.com	✓
fastmail.com	✓
freemail.hu	✓
mail.ru	✓
naver.com	✓
rediffmail.com	✓
yahoo.com	✓
zoho.in	✓
daum.net	✓
interia.pl	✓
inbox.lv	✓
icloud.com	✓
runbox.com	✓
seznam.cz	✓
o2.pl	×
wp.pl	×
sohu.com	×
t-online.de	×
excite.com	×
gmail.com	✓
outlook.com	✓

STARTTLS

- 23 mail providers support STARTTLS

Popular Email Service Providers' DANE Support

Total 29

Mail Provider	TLSA Request	Validation
mail.com	✓	▲
comcast.net	✓	✓
gmx.com	✓	✓
tutanota.com	✓	▲
mynet.com	×	×
sapo.pt	×	×
sina.com	×	×
protonmail.com	×	×
aol.com	×	×
fastmail.com	×	×
freemail.hu	×	×
mail.ru	×	×
naver.com	×	×
rediffmail.com	×	×
yahoo.com	×	×
zoho.in	×	×
daum.net	×	×
interia.pl	×	×
inbox.lv	×	×
icloud.com	×	×
runbox.com	×	×
seznam.cz	×	×
o2.pl	×	×
wp.pl	×	×
sohu.com	×	×
t-online.de	×	×
excite.com	×	×
gmail.com	×	×
outlook.com	×	×

DANE

- 4 mail providers fetch TLSA records

Popular Email Service Providers' DANE Support

Total 29

Mail Provider	TLSA Request	Validation
mail.com	✓	▲
comcast.net	✓	✓
gmx.com	✓	✓
tutanota.com	✓	▲
mynet.com	×	×
sapo.pt	×	×
sina.com	×	×
protonmail.com	×	×
aol.com	×	×
fastmail.com	×	×
freemail.hu	×	×
mail.ru	×	×
naver.com	×	×
rediffmail.com	×	×
yahoo.com	×	×
zoho.in	×	×
daum.net	×	×
interia.pl	×	×
inbox.lv	×	×
icloud.com	×	×
runbox.com	×	×
seznam.cz	×	×
o2.pl	×	×
wp.pl	×	×
sohu.com	×	×
t-online.de	×	×
excite.com	×	×
gmail.com	×	×
outlook.com	×	×

DANE

- 4 mail providers fetch TLSA records
- 2 providers correctly validate all fields in a TLSA record

Popular Email Service Providers' DANE Support

Total 29

Mail Provider	TLSA Request	Validation
mail.com	✓	▲
comcast.net	✓	✓
gmx.com	✓	✓
tutanota.com	✓	▲
mynet.com	×	×
sapo.pt	×	×
sina.com	×	×
protonmail.com	×	×
aol.com	×	×
fastmail.com	×	×
freemail.hu	×	×
mail.ru	×	×
naver.com	×	×
rediffmail.com	×	×
yahoo.com	×	×
zoho.in	×	×
daum.net	×	×
interia.pl	×	×
inbox.lv	×	×
icloud.com	×	×
runbox.com	×	×
seznam.cz	×	×
o2.pl	×	×
wp.pl	×	×
sohu.com	×	×
t-online.de	×	×
excite.com	×	×
gmail.com	×	×
outlook.com	×	×

DANE

- 4 mail providers fetch TLSA records
- 2 providers correctly validate all fields in a TLSA record
- Other 2 providers do not validate one field correctly

Popular Email Service Providers' DANE Support

DANE support in the popular email service providers is still in an early stage

Outline of Analysis

Server-side

DANE Deployment

DANE Management

Client-side

Email Service Provider

MTA & DNS Software

Popular MTA and DNS software

MTA Software

MTA Software	STARTTLS Support	DANE Support
Postfix 3.4.7	✓	✓
Exim 4.92.3	✓	✓
sendmail 8.15.2	✓	×
Exchange Server 2019	✓	×

All support STARTTLS
2 support DANE

Popular MTA and DNS software

MTA Software

MTA Software	STARTTLS Support	DANE Support
Postfix 3.4.7	✓	✓
Exim 4.92.3	✓	✓
sendmail 8.15.2	✓	×
Exchange Server 2019	✓	×

All support STARTTLS
2 support DANE

DNS Software

DNS Software	DNSSEC Support	TLSA Support
BIND9 9.14.7	✓	✓
PowerDNS 4.2.0	✓	✓
Microsoft DNS	✓	✓
Simple DNS Plus 8.0.110	✓	✓
NSD 4.2.2	✓	✓
KnotDNS 2.9.0	✓	✓
YADIFA 2.3.9	✓	✓
Unbound 1.9.4	✓	✓
djbdns 1.05	×	×
MaraDNS 3.4.01	×	×
posadis 0.60.6	×	×

8 support DNSSEC
TLSA

Popular MTA and DNS software

DANE support in the popular MTA and DNS programs is pervasive

Conclusion

- Presented a longitudinal and comprehensive study of the DANE ecosystem in SMTP

- Server-side: DANE deployment is scarce but increasing
  - 1/3 of TLSA records cannot be validated due to missing or incorrect DNSSEC records
  - 3.68% of the certificates are inconsistent with their TLSA records

- Client-side: DANE deployment is also rare
  - Only 4 email service providers support DANE out of 29 popular email providers
  - 2 MTA and 8 DNS programs support DANE

- Datasets & source code
  - https://dane-study.github.io/

Thank you!

Any questions?

Hyeonmin Lee

hmlee@mmlab.snu.ac.kr

Appendix

DANE Deployment – Daily Dataset

Domain data from OpenINTEL (https://openintel.nl/)

TLD	Generic TLD			Country-code TLD	
	.com	.org	.net	.nl	.se
# of scanned domains	72.9M	7.4M	6.1M	4.3M	0.86M
Interval	2017-10-22 ~ 2019-10-31				
Period	Every day				

DANE Management – Hourly Dataset

Vantage Point	Oregon	Virginia	São Paulo	Paris	Sydney
# of TLSA records (of last snapshot)	7.9K	7.9K	7.9K	7.9K	7.9K
# of Certificates (of last snapshot)	7.3K	7.3K	7.3K	7.3K	7.2K
Interval	2019-07-11 ~ 2019-10-31				
Period	Every Hour				